# Pretty Handy Degree

Nate Foster Cornell University



Prelude

#### Disclaimer: A Survivor's Story



#### ... Geographically Biased



#### ... And A Personal Story



#### Acknowledgments



Kim Bruce



Phillip Guo



Nick Feamster



Matt Might



Andrew Myers



Benjamin Pierce



Yannis Smaragdakis



Ross Tate

#### Acknowledgments



Why do a PhD?





JANUARY 14, 2014, 8:46 AM | Comment

#### Daily Report: With \$3.2 Billion Deal for Nest, Google Makes a Play for Your Home

By THE NEW YORK TIMES



Google, which dominates much of life on the Internet, has been trying to expand beyond computers and telephones to living rooms, cars and bodies, Claire Cain Miller reports. It made its way a bit further into people's homes on Monday when it agreed to pay \$3.2 billion in cash for Nest Labs, which makes Internet-connected devices like thermostats and smoke alarms.



Nest, which was started in 2010 by Tony Fadell and Matt Rogers, members of the teams that built the iPhone and iPod at Apple, will continue to operate independently under its own brand and expand its portfolio of connected versions of what it calls "unloved but important devices in the home."

JANUARY 14, 2014, 8:46 AM DComment

Bits

#### Daily Report: With \$3.2 Billion Deal for Nest, Google Makes a Play for Your Home By THE NEW YORK TIMES



Google, which dominates much of life on the Internet, has been trying to expand beyond computers and telephones to living rooms, cars and bodies, Claire Cain Miller reports. It made its way a bit further into people's homes on Monday when it agreed to pay \$3.2 billion in cash for Nest Labs, which makes Internet-connected devices like thermostats and smoke alarms.

Daily Repor

Nest, which was started in 2010 by Tony Fadeli and Matt Rogers, members of the teams that built the iPhone and iPod at Apple, will continue to operate independently under its own brand and expand its portfolio of connected versions of what it calls "unloved but important devices in the home."





Nobody will ever call you "doctor" except your mom...

... you will get asked "when are you finally going to graduate?"



Nobody will ever call you "doctor" except your mom...

#### ... you will get asked "when are you finally going to graduate?"



#### Undergrad Was Fun



#### Undergrad Was Fun



#### Undergrad Was Fun



#### Become a Professor



#### Become a Professor



#### Become a Professor



#### Opens Opportunities

#### **Opens Opportunities**



## Opens Opportunities



- Universities
- Civil service
- National labs
- Corporate research labs
- Research and development
- Advanced engineering

#### Freedom!



# Work on Big Problems

Many grand challenges:

- Verification
- Security and Privacy
- Fault tolerance
- Distributed computing
- Energy-efficient computing
- Systems biology

• . . .

A lot of them require the tools and techniques of the POPL community!



### Work on Big Problems



# What is a PhD?

**High school:** basic knowledge of a broad range of topics

High school: basic knowledge of a broad range of topicsUndergrad: broad knowledge and specialization in a field

**High school:** basic knowledge of a broad range of topics

**Undergrad:** broad knowledge and specialization in a field

**Professional:** advanced knowledge and practical skills

**High school:** basic knowledge **I** of a broad range of topics

**Undergrad:** broad knowledge and specialization in a field

**Professional:** advanced knowledge and practical skills

Well-defined requirements High rate of completion

**High school:** basic knowledge of a broad range of topics

**Undergrad:** broad knowledge and specialization in a field

**Professional:** advanced knowledge and practical skills

**PhD:** advanced knowledge + a research contribution

Well-defined requirements High rate of completion
# Comparing Degrees

**High school:** basic knowledge of a broad range of topics

**Undergrad:** broad knowledge and specialization in a field

**Professional:** advanced knowledge and practical skills

**PhD:** advanced knowledge + a research contribution



#### Transformation

#### Transformation



# How to do a PhD

#### Step 0: Pick an Institution





# Step 0: Pick an Institution

#### Very important:

- Advisor
- Opportunity
- Peers

#### Typically less important:

- Finances
- Institution
- Location

#### Advice:

- Apply to the top programs in CS and your area
- Talk to current students
- Look at recent results

#### MARRIAGE vs. The Ph.D.

	Marriage	<u>Ph.D.</u>
Typical Length:	7.5 years	7 years
Begins with:	A proposal	A thesis proposal
Culminates in a ceremony where you walk down an aisle dressed in a gown:		
Usually entered into by:	Foolish young people in love	Foolish young people without a job
50% end in:	Bitter divorce	Bitter remorse
Involves exchange of:	Vows	Know-how
Until death do you part?	If you're lucky	If you're lazy

#### Typical requirements

- Demonstrate broad knowledge of Computer
   Science at the advanced undergrad level
- Demonstrate specific
  knowledge of your field
- Often assessed as a set of written/oral exams



#### Typical requirements

- Demonstrate broad knowledge of Computer
   Science at the advanced undergrad level
- Demonstrate specific
  knowledge of your field
- Often assessed as a set of written/oral exams



Designed to be straightforward, but can be difficult when juggling living in a new town, teaching, fellowships, research, etc.

#### Typical requirements

- Demonstrate broad knowledge of Computer
   Science at the advanced undergrad level
- Demonstrate specific
  knowledge of your field
- Often assessed as a set of written/oral exams



Designed to be straightforward, but can be difficult when juggling living in a new town, teaching, fellowships, research, etc.

#### My emotions: extreme stress!

Ideally, can get involved with research early on...

Ideally, can get involved with research early on...

...many advisors will point junior students down a clear path

Ideally, can get involved with research early on...

...many advisors will point junior students down a clear path

#### Combinators for Bi-Directional Tree Transformations: A Linguistic Approach to the View Update Problem

J. NATHAN FOSTER University of Pennsylvania MICHAEL B. GREENWALD Bell Labs, Lucent Technologies JONATHAN T. MOORE University of Pennsylvania BENJAMIN C. PIERCE University of Pennsylvania ALAN SCHMITT INRIA Rhône-Alpes

We propose a novel approach to the view spilate problem for trae-structured data: a domainspecific programming language in which all expressions denote bi-directional transformations on trees. In one direction, these transformations—dubbed ienzer—map a "concrete" tree into a simplified "sharinet view"; in the other, they map a modified abstract view, (appther with the original concrete tree, to a correspondingly modified concrete tree. Our design emphasizes both robustness and case of use, guaranteeing strong self-behavedness and totality properties for welltyped leaves.

We begin by identifying a natural mathematical space of well-behaved bi-directional transformations over arbitrary structures, studying definednose and continuity in this setting. We then instantiate this semantic framework in the form of a collection of less combinators that can be assembled to describe bi-directional transformations on trees. These combinators include familiar constructs from functional programming (composition, mapping, projection, conditional, recursion) together with some novel primitives for manipulating trees (uplitting, prusing, orgying, merging, etc.). We illustrate the expressiveness of these combinators by developing a number of bi-directional lin-spectrosing transformations as derived forms. An extended example shows how our combinators can be used to define a less that translates between a native HTML representation of browser bookmarks and a generic abstract bookmark format.

Categories and Subject Descriptors: D.3.2 [Programming Languages]: Language Classifications—Specialized application languages

General Terms: Languages

Additional Key Words and Phrases: Bi-directional programming, Harmony, XML, lenses, view update problem

Permission to make digital/hard copy of all or part of this material without for for personal or classroom use provided that the copies are not made or distributed for profit or commercial advantage, the ACM copyright/server action, the title of the publication, and its data appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a for. (9) 2007 ACM XXX-XXXX XXXX 4XXXX 4XXXX

ACM Transactions on Programming Languages and Systems, Vol. TBD, No. TDD, Month Year, Pages 1-77

Ideally, can get involved with research early on...

...many advisors will point junior students down a clear path

Goal: a taste of research

- Model: apprenticeship
- Role: provide thrust

**My emotions:** excitement and perhaps a bit of shell shock

#### Combinators for Bi-Directional Tree Transformations: A Linguistic Approach to the View Update Problem J. NATHAN FOSTER University of Pennsylvania MICHAEL B. GREENWALD Bell Labs, Lucent Technologies JONATHAN T. MOORE University of Pennsylvania BENJAMIN C. PIERCE University of Pennsylvania ALAN SCHMITT INRIA Rhône-Alpes ose a novel approach to the view update problem for tree-structured data: a dom specific programming language in which all expressions denote bi-directional transformations or trees. In one direction, these transformations—dubbed lensers—map a "concrete" tree into a implified "abstract view"; in the other, they map a modified abstract view, together with the inal concrete tree, to a correspondingly modified concrete tree. Our design emphasizes bot ubustness and case of use, guaranteeing strong well-behavedness and totality properties for well We begin by identifying a natural mathematical space of well-behaved bi-directional transf ations over arbitrary structures, studying definedness and continuity in this setting. We then stantiate this semantic framework in the form of a collection of lens combinators that can be enhied to describe bi-directional transformations on trees. These combinators include familia acts from functional programming (composition, mapping, projection, cond ion) together with some novel primitives for manipulating trees (splitting, pruning, copying serging, etc.). We illustrate the expressiveness of these combinators by developing a number of i-directional list-processing transformations as derived forms. An extended example shows how nators can be used to define a lens that translates between a native HTML r of browser bookmarks and a generic abstract bookmark format. Categories and Subject Descriptors: D.3.2 (Programming Languages): Language tions-Specialized application languages General Terms: Languages Additional Key Words and Phrases: Bi-directional programming, Harmony, XML, le update problem to make digital/hard copy of all or part of this material without fee for pe or classroom use provided that the copies are not made or distributed for profit or commercial advantage, the ACM copyright/server notice, the title of the publication, and its date appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, post on servers, or to redistribute to lists requires prior specific permission and/or a fee D 2007 ACM XXX-XXX/XX/XXXX-XXXX 8XX.XX ctions on Programming Languages and Systems, Vol. TBD, No. TDD, Month Year, Pages 1-

### Step 3: Iterate

Then one repeats the process (ideally several times) showing that the first result was not a fluke

#### Step 3: Iterate

Then one repeats the process (ideally several times) showing that the first result was not a fluke

#### Boomerang: Resourceful Lenses for String Data

Aaron Bohannon

University of University of Pennsylvania

J. Nathan Foster Benjamin C. Pierce Alexandre Pilkiewicz Alan Schmitt. Ecele Polytechnique DNRIA Ridne-Alpen

#### Abstract

A dow is a bidirectional program. When read hows left to right, it denotes an ordinary function that maps imputs to compute. When read from right to left, it denotes an "update translator" that takes an imput together with an updated output and produces a new input that effects the update. Many variants of this idea have been explored in the lineature, but none deal fully with ordered data. If, for example mail and in

In this matrix, but note that they with ordered data. It, for example, in a plate changes the other of a last in the corput, the them in the matrix of the chanks of the input that generated them can be matrixed. Surfage to law or correspond data. We attack this patholin in the content of their networks, then one of the standard of the content of their networks, based on familiar operations on regular transformed data type. We fore per-pages a collection of their networks and a standard data type. We there per-pages a collection of their networks of the standard data on familiar operations on regular transformed on regular experi-tions. Known-out and with a spee system based on regular exper-tions. Not not design a new sensatic space of distingues junctions additional combination for marking "resolutions" index we do-solution the design a new sensatic space of distingues junctions additional combination for marking "resolutions" interva-additories and pergramments the efficiences of the specific distings and index ourse word Biocenessage to half transforms in the sense of world datas formate including the Swindry of resourced advection of these to exolute the share index of the standard or advection of these to exolute the share index of the standard ourset and wings to any to an output of resourced blocks. We formation the sensetial property of resourced blocks — the pervised by standard properties of datas in the standard and the standard and approximation in the standard of datas in the standard and the standard approximation in the standard of datas in the standard and the standard pervised by standard pergention of datas in the standard and the standard and pervised by standard data pergention of datas in the standard and the standard and pervised by standard pergention of datas in the standard and the standard and the standard and the standard and pervised by standard pergention of datas in the standard and the stand

ionaly studied properties of lenses turn out to have compact actenizations in this space.

Categories and Subject Descriptors D.3.2 (Programming Lan-proper): Language Classifications-Specialized application In-

General Terms Languages, Design, Theory Erwards Bidrectional languages, lemes, view splate problem regular string translaters, regular types

#### 1. Introduction

"The art of progress is to preserve order and change and to preserve change anid order." — A N Whitehead

Most of the time, we use programs in just one direction, from input to output. But sometimes, having computed an output, we need to Lesses The language described in this paper is an ext

n in make digital or bad angine of all or part of this work for personal or one is general without the postful disc capits are not made to discriming a concernial discontage and here inspire here this notion and the fall distance (page, To any otherwise, in regulital, to particular terms in a collabilithate gaver, prior specific permission and/or a first.

In affirits update this strappt and then "calculate backwards" to find a correspondingly updated tipst. The position of writing cash hid excitant backwardsen actions are studiented of domains, includ-ing data converters and synchronizers, pursues and perty printers picken and updaters, stratum ofdate, constant maritaners for per interfaces, and, of course, in datab the view apdate problem. Our own study of hidroctional transfit mations is motivated by their application in a generic synchronizy tion framework, called Harmony, where they are used to nise henoregeneous data formats against each other (Pierce et a 2006; Foster et al. 2087a). The naive way to write a bidirectional trans-

ply to write two separate functions is any language you like and check (by hand) that they fit together in some appropriate sense-e.g., that composing them yields the identity function. However, this approach is unsatisfying for all but the simplest example For one thing, verifying that the two functions fit together in t For our image programmers and a second se

programming language. It a bidirectional langu-sion, when read from left to right, denotes a furand to complete when and first applies to the same expression denotes a function mapping as sphere subject support of the same expression of the same expression of the same regional lepse to an appropriately sphere when the same expression of parts provide the same expression of the same expression of parts provide the same expression of the same expression of parts provide the same expression of the same expression. on design the language to guerantee it. Many different Hidroctional languages I

ing constraint instantions (Malerian 1998), pickly on Kristophy 2010), coloridating projection parts (Donion or 2000), Killer (Marcel and Kristophy 2006), Niller (Veller 1), Schler (Kristowika and Kristophy 2006), Philit (Veller 2007), and benefits (Kristowika et al. 2007). The strength for all these languages for in streling a believe implementation and relativity making strengt press in representation and relativity. en about the joint behavior address under which they o

ious presentation on lonses (Poster et al. 2007): lanses here." Among the bidirectional languages listed a

from an element of A using a result function instand of a special element II and using par. Second, as we are not advant to reconstant, see take the commerces, of inter-

### Step 3: Iterate

Then one repeats the process (ideally several times) showing that the first result was not a fluke

**Goal:** demonstrate ability to repeatedly produce high-quality research results

Model: junior partner Role: discover technical insights My emotions: frustration

<text><section-header><section-header><section-header><text><text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text></text></section-header></section-header></section-header></text>	<text><text><text><text><text><text><text><text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text>	Aaron Bohannon University of	J. Nathan Foster University of	Benjamin C Universit	. Pierce	Alexandre Pilkiewicz École Polytechnique	Alan Schmitt INRIA Ridse-Alpes
<text><text><text><text><text><text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text></text></text></text></text></text>	<text><text><text><text><text><text><text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text></text></text></text></text></text></text>	Penniphone	Petrophana	Pennyts	ursa.		
When it for the task, we can program it per contractions, then input, it output, But constitues, hereing computed in output, we need to be compared as the second secon	State of basis, we are proposed in part and electron, but may be in output. But sometimes, hering computed in output, we need to be output. But sometimes, hering computed in output, we need to be and the source of the source of all or part of this web for presentation. If the source of the source of the source of the basis deversible of the source of all or part of this web for presentation. If the source of the source of the source of the source of the basis deversible of the source of the source of the source of the source of the source of the source of the source of the source of the source of the source of the basis of the source o	Abstract A den in a following of a denome an ordinary fue denome an ordinary fue of the ordinary for the ordinary per imperior which and ordinary for interaction of the ordinary of the ordinary for the ordinary method ordinary for the ordinary for the ordinary for the ordinary per a collection of the per a collection of the per a method data format in the per collection of the per a collection of the collection of the per a method of the the collection of the per a collection of the per a method data format is the per a collection of the per a collection of the collection of the per a method of the the collection of the per a collection of the per a collection of the collection of the per a co	program. When sead free clean that maps inputs to end output and producers indication of the indication of output and producers of a law in the output, of of the input the generator of the input the generator of the input the generator is the context of Midland produced and the sys- temical arring laws used in a spectra strain of the sec- tion of a second strain optimized arrival second of in- stration of the second second of the system based out- in spectra system based out- in the system based out- inguine tradewide the sys- tematical "second second second other at al. (2007b) with a discontext of these prior discontexts of the imputs of the system. Socialised of the system of prior of prior discontexts in the preserve and the second second second second second second second second second second second second second second second second second second second se	a left to right, support. When any every the support of that takes any new input that the input that of the support of the sup	be able to a convergence of the second ing data, pickless of the second be shown into the second be shown into the second Distribution of the second Distribution Distribution of the second Distribution of the second Distribution Distribution of the second Distribution of the second Distribution Distribution of the second Distribution of	a qudate this surget and then "a outdary hydrated input. The pri- transformations arises in a mit commenters and synchronizons, and capacities, structure addates finders, and, of quadrations, and capacities, structure addates finders, and, of surgets and optime problem. Our overs stud as motivated by their application arrows, called Batmony, when migneture date. Structure again state with a white a bidirection in the way to when a bidirection in the way to when a bidirection the two superate functions in a structure way to waite functions in a structure of the superstate of composing them yields the 1 biding, workfung their the two fu- misms neutrons requesting shores for maintenance singletimes. Noti- ther the lapet and support of paperalle first a two functions in a structure mapping and the support of the the lapet and support of the simulation requesting shores in the paperalle first to be fulfage a too to any holessing of the support of the simulation request a signation of the lapet of the signation of the simulation request a signation of the lapet of the signation of the simulation work deglescates of the dimension work deglescates of the dimension work deglescates of the dimension work deglescates of the dimension and the signation of the simulation and the signation of the simulation and the simulation of the simulation and the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the simulation of the	docknet backwards" to faid hilters of writing cash bid- hilters of domains, includ- instant of domains, includ- seres and protype pertors, constraint maintainers in a generic operation of the sec- sion of the second transformer they are used to synchronize they are used to synchronize ones appropriate second transformer they are used to synchronize the second second transformer to the simplest camples, norther for hypothesis second- instruction will embedy the functions will embedy the functions will embed the functions will embed by the functions of the synchronized of imparts of the synchronized of space sectors property, in a synchronized by pertor- izions in structure property, the synchronized by the synchronized of the synchronized by the synchronized by the synchronized of the synchronized by the synchronized by the synchronized of synchronized by the synchronized of the synchronized by the synchronized by the synchronized by the sheet synchronized by the s
Persistin to nale diplic or had copies of all or part of lits works for present or formers or a parent extinct for the probability of the copies are not nait or distributed from the simulation. Plant is the backle size of the size of the size of the form the simulation of the size of the size of the size of the form the simulation. The size of the s	Persistin to nale diplic or had copies of all or per of its work for personal or frameware at parent without the discussion of the copies of the copies of the frameware at personal filter operation of the copies of the copies of the frameware at personal of the copies of the copies of the copies of the frameware at personal of the copies of the copies of the frameware at personal of the copies of the copies of the frameware at personal of the copies of the copies of the frameware at personal of the frameware at personal of the frameware at personal distance of the frameware at personal of the frameware	Most of the time, we use p to output. But sometimes,	rognens in just one directi Auring computed an outp	ion, from input set, we need to	Lenses our peri- basic len	The language described in th ious presentation on leases (Pr sea here." Aerong the bidirection	is paper is an extension of nier et al. 2007()—called ral languages listed above,
		Percisian to nato digital ar ha dataman ter is genited without for godi or summerial alonga or far ton app. To any suffersi to line, equiper prior quarks prior to line, equiper prior quarks prior (2010) (8). Inserty 7-10, 2008. (2010) (8). 2008. ACM 978-1-0 (2010) (8).	of cogines of all or part of Nos on the provided that cogine are not a cracel that cogine here this order of the computation, for part on a series within and/or a No. In Proceedings Collification, USA, and series of collection,	nia las presenta ar sulo or distributed noi de l'al-citation a arte estimitation	<sup>1</sup> Readors foremants from at d defined to tions cells initiality for	familiar with the original prevented from the bandle situations where an isomet of A using a owner barchine ment OI and using park. Second, an a treatment, we take the composer of the defining bernes with partial ex. Finally, we take the behavioral to	m will holice usine millior dif- demonst of C must be result instant of concluding C with a wear set as considering lenses as of instants to be total fine- compression and establishese any any of the fundamental area a part of the fundamental

Boomerang: Resourceful Lenses for String Data

## Step 4: Independence

Eventually, begin to show leadership and break ground in new directions

### Step 4: Independence

#### Eventually, begin to show leadership and break ground in new directions

#### Updatable Security Views

#### J. Nathan Foster Benjamin C. Pierce Steve Zdancewic University of Pennsylvania

#### Abstract

Security views are a flexible and effective mechanism for allowing untrusted users to access source data directly, they are instead presided with a restricted view, from which all unfidential information has been removed. The program that penerates the view effectively embodies a confidentiality policy for the underlying source data. However, this ap-proach has a significant drawback: it prevents users from updating the data in the view.

in two directions: mad from left to right, they map sources to views; from right to left, they map updated views back to updated sources. Wesever, existing hidrectional languager do not deal adequately with security. In particular, they do not provide a way to ensure the integrity of source data as it is manipulated by untrusted users of the view.

We prepare a nevel framework of secure lenses that addresses these shorecomings. We enrich the types of basic lenses with equivalence relations capturing notions of confidestiality and integrity, and formulate the ecsential security conditions as non-interference properties. We then instanti-are this framework in the domain of string transformations, developing syntax for bidirectional string combinators with security-annotated regular expressions as their types.

#### 1. Introduction

Security views are a widely used mechanism for controlling access to confidential information in databases and other systems that manage structured information. By forcing  $L_{pet}(l_{pet}v|x) = v$  (PUIG(1)) users to access data via views that only expose public information, data administrations ensure that secrets will not be leaked, even if the users mishandle the data or are malicious. Security views are robust, making it impossible for users. The ger function defines the view and is a total function both the source data hidden by the view, and they are initial to N. There are two functions that handle updates: within since they are implemented as arbitrary programs, the put function takes an updated V and the original S and fexible: since they are implemented as arbitrary programs, they can be used to enforce extremely fine-grained access control policies. However, they are not usually updatable-and for good nuscen! Propagating updates to views made by untracted users can, in general, after the source data, including the parts that are hidden by the view. the original (it fills in any source data that is not reflected in the view with default values).

Sill, there are many applications in which having a mechanism for reliably updating security views would be ty views are a fexible and effective mechanism for tiling access to confidential information. Bather than laborative data sharing system based on Wikipedia that is used by members of the intelligence community. The data stored in Intelligedia is classified at the granularity of whole documents, but many documents actually contain a mixture of highly classified and less-classified data. In order to give users with low clearances access to the portions of documents they have sufficient clearance to see, documents often have to be negraded; i.e., the highly classified parts To address the "view spelate problem" in general, a number of bidirectional languages have been proposed. Pro-grams in these languages -often called lenses--can be rent. about a wiki), we would like the users of these views to be able to make updates-e.g., to correct errors or add new information-and have their changes he propagated back to the original document. In general, for a view to be updatable, the program that

generates it needs to be hidroctional. That is, it must not only be able to transform sources to views but also to map updated views back to updated sources. In previous work, we and many others have proposed a family of language for describing bidirectional transformations, often called fenary [19], [8], [7], [21], [37], [41], [26], [9], [24], [35], [17], [23], [30], [28], Formally, a lens l mapping between a set S of "source" structures and a set V of "views" comprises three functions.

 $L_{BH} \in S \longrightarrow V$ I put  $\in V \longrightarrow S \longrightarrow V$ Lorente  $\in V \longrightarrow S$ 

(PVTG(1))

Last (Lonate v) = v (CREATEGET) Lpst (Lpst s) s = s (OUTPUT) weaves them together to yield a correspondingly modified S, while the owner function handles the special case where we need to compute an S from a V but have no S to use an

## Step 4: Independence

Eventually, begin to show leadership and break ground in new directions

Goal: demonstrate independence and maturity as a researcher Model: colleague Role: finding the question My emotions: excitement

#### Updatable Security Views

#### J. Nathan Foster Benjamin C. Pierce Steve Zdancewie University of Pennsylvania

#### Abstract

Security views one a facilite and effective mechanism for controlling access to confidential information, Bather than allowing methods access source data directly, they are instead presided with a restricted view, from which all confidential information has been removed. The program that generates the view effectively embeddes a confidentially policy for the underlying source data. However, this appreach has a significant denoback: it prevents source from uplacing the data in the view.

To address the "view update problem" in general, a number of bidirectional languages have been proposed. Programs in these languages, other collide languages the in two divections: mud from left as right, they may sources to views: from right to left, they may reduced views back to updated sources. However, existing bidirectional languages do not doal adequately with security. In particular, they do not provide a way to ensure the integrity of source data ar it is multiplated by attracted source of the view.

We prepare a never framework of secure benuss that addresses these shorecomings. We works the types of basic benues with equivalence relations capturing netions of confidentiality and bacgoing, and formulate the eccentral security conditions as non-interference properties. We show instantate this foamwork in the domain of string transformations, developing synam (for biddoccional string transformations, developing synam copression as their types.

#### 1. Introduction

Security views are a widely used mechanism for controlling access to confidential information in databases and other systems that manage excutated information. By forcing users to access data via views that only expose public information, data administrators moure that secrets will not be leaked, even if the users mishandle the data or are malicion. Security views are robust, making it impossible for users to leak the source data hidden by the view, and they are facilite; since they are inplemented as arbitrary program, they can be used to enforce extremely the-grained access control splicies. However, they are not usually updatable and for good trason? Propagning updates to views made by untrusted users can, in general, also the source data, including the pars that are bidden by view.

Sill, there are many applications in which having a machanism for reliably updating security views would be relatenetly used. For example, consider historilippelia, a citiable of the statistical security of the data used by members of the intelligence community. The data started is having documents actually contains a minitare of highly classified and laws deastiled data. In order to give users with law classified data. In order to give users with law classified data. In order to documents day have classified data. In order to documents day have sufficient dentance in sec. As an evolution of the terms with law classified data. In order to documents day have sufficient dentance in sec. As an evolution for the ensuel or reducted, having behind a resolution document—as occurity view!—that can be reclassified at a lawer level of clasmone. Of course (sizes or doable to which, we would like the users of these views to the able to make update—a, to correct ensues are also to able to make update—a, to correct terms or add area to easily and the clasmone. The populated back to the data to make update—a, to correct ensues and they are order to make update—a, to correct ensues or add the order of the population of the population of the order.

In general, for a view to be updatable, the program that generates it needs to be biddencional. That is, it must net only be able to transform sources to views but also to map updated views back to updated sources. In previous work, we and many others have proposed a family of languages for describing bidirectional transformations, other called leases (198, 1981, 171, 1971), (1971, 1971, 1971, 1971, 1971, (1971, 1973, 1987, 1987, 1971, 1971, 1971, 1971, 1971, (1971, 1973, 1987, 1987, 1971, 1971, 1971, 1971, 1971, (1971, 1973, 1987, 1987, 1971, 1971, 1971, 1971, 1971, (1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, (1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, (1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, (1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, (1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, (1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, 1971, (1971, 1

Law	e	8		¥	
Lput	e	v	_	8	$\rightarrow V$
nuit	e	v		8	

that only "round-trigging" laws for every  $s \in S$  and  $v \in V$ .  $L_{pet}(L_{pet}v s) = v$  (PUTCET)  $L_{pet}(L_{pet}v s) = v$  (PUTCET)  $L_{pet}(L_{pet}s) = v$  (PUTCET)  $L_{pet}(L_{pet}s) = s$  (PUTET) The get function defines the view and is a total function from S to V. There are two functions that bandle updates: the put function takes an updated V and the original S and weaves from together to yield a correspondingly modified S, while the overare function handles the update of S on the si

the original (it fills in any source data that is not reflected in the view with default values).

## Step 5: End-Game

When it is time to move on...

- Form a committee
- Propose the thesis
- Write the dissertation
- Network and give talks
- Find a job

## Step 5: End-Game

When it is time to move on...

- Form a committee
- Propose the thesis
- Write the dissertation
- Network and give talks
- Find a job



John Nathan Foster

## Step 5: End-Game

When it is time to move on...

- Form a committee
- Propose the thesis
- Write the dissertation
- Network and give talks
- Find a job

My emotions: relief and exhaustion



A wonderful time to engage deeply with research

A wonderful time to engage deeply with research

+ Lots of unstructured time

A wonderful time to engage deeply with research

- + Lots of unstructured time
- + Few responsibilities

- A wonderful time to engage deeply with research
- + Lots of unstructured time
- + Few responsibilities
- + Substantial freedom

A wonderful time to engage deeply with research

- + Lots of unstructured time
- + Few responsibilities
- + Substantial freedom
- (Relative) poverty

A wonderful time to engage deeply with research

- + Lots of unstructured time
- + Few responsibilities
- + Substantial freedom
- (Relative) poverty
- Not much respect

A wonderful time to engage deeply with research

- + Lots of unstructured time
- + Few responsibilities
- + Substantial freedom
- (Relative) poverty
- Not much respect

"Don't make fun of grad students; they've just made a terrible life choice"

–The Simpsons

A wonderful time to engage deeply with research

- + Lots of unstructured time
- + Few responsibilities
- + Substantial freedom
- (Relative) poverty
- Not much respect

"Don't make fun of grad students; they've just made a terrible life choice"

–The Simpsons

- Can be difficult to get distance from work

- A wonderful time to engage deeply with research
- + Lots of unstructured time
- + Few responsibilities
- + Substantial freedom
- (Relative) poverty
- Not much respect

"Don't make fun of grad students; they've just made a terrible life choice" –The Simpsons

- Can be difficult to get distance from work



Thank you!