Today's Menu

What Every ~~Computer Scientist~~ Human Should Know about Security

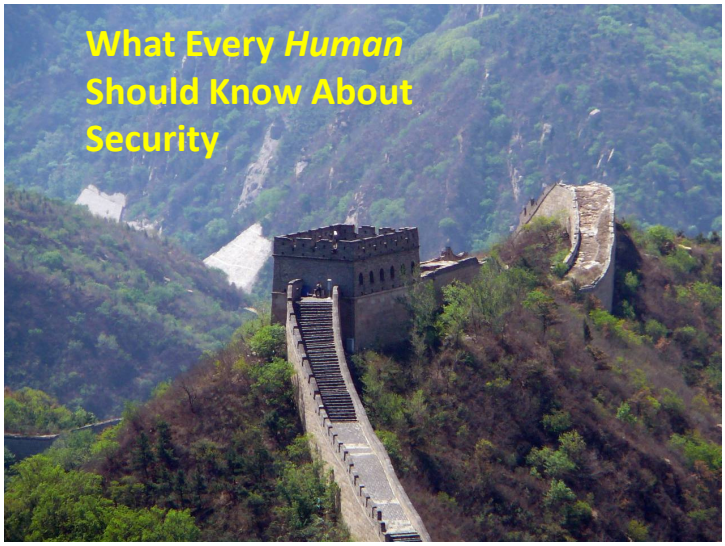
GuardRails

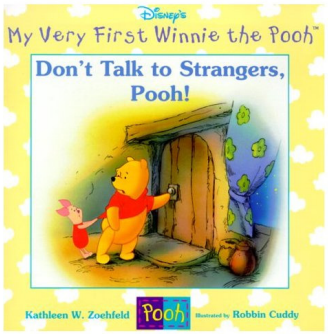
Jonathan Burket (BACS 2)
Patrick Mutchler (BSCS 4)
Michael Weaver (BSCS 4)
Muzzammil Zaveri (BACS 4)

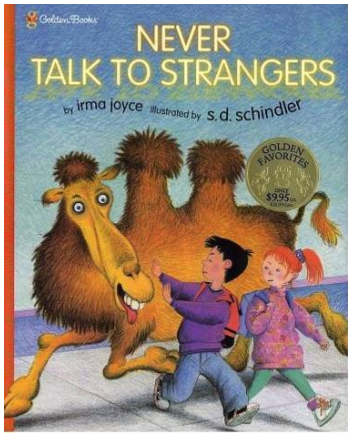
Efficient Secure Computation

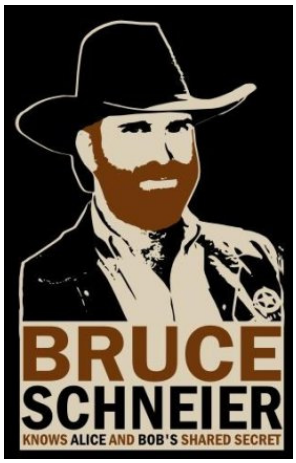
Yan Huang (CS PhD)
Yikan Chen (CpE PhD)
Jerry Ye (BSCS 3)
Samee Zahur (CS PhD)

I'm looking for new students for the summer for both projects (and other ideas)!

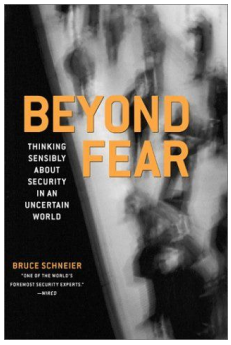


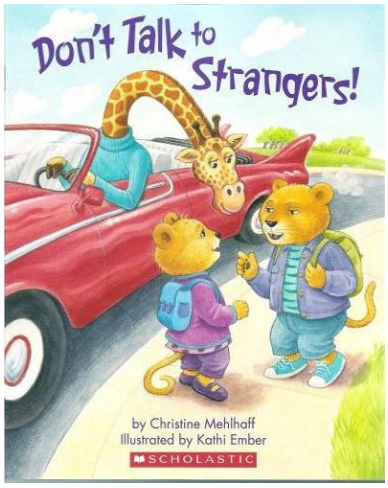






"Many children are taught never to talk to strangers, an **extreme precaution with minimal security benefit**."





"Emma Lion loves to make new friends, but Mama tells her to be careful and never talk to strangers. Emma sees new people to meet everywhere she goes. **How will she know who is a stranger**?"

Security

- Technical questions
  - Figuring out who is not a "stranger" (***authentication***)
  - Controlling access to resources (***protection*** and ***authorization***)
- Value judgments
  - Managing risk vs. benefit (***policy***)
- Deterrents
  - If you get caught, bad things happen to you

Protecting assets from misuse

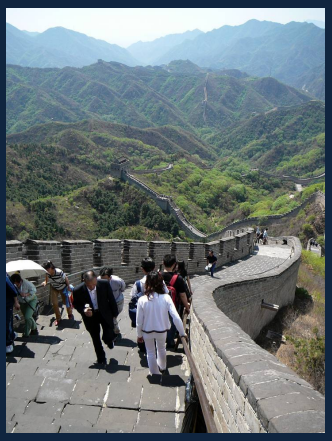
Computer Security

Study of computing systems in the presence of *adversaries*

about what happens when people don't follow the rules

Quiz

Authentication, Protection, Authorization, Policy, or Deterrent?



Authentication, Protection, Authorization, Policy, or Deterrent?

Charlottesville Airport, Dec 2001

Authentication, Protection, Authorization, Policy, or Deterrent?

British Parliament, Dec 2007

A (Nearly) Painless Solution to Web Application Security

Jonathan Burket, Patrick Mutchler,
Michael Weaver, Muzzammil Zaveri

Web Security is Annoying and Tedious

Access Control

```
if include_subprojects && !active_children.empty?
    ids = [id] + active_children.collect {|c| c.id}
        conditions = ["#{Project.table_name}.id IN (#{ids.join(',')})"]
                AND #{Project.visible_by}"]
```

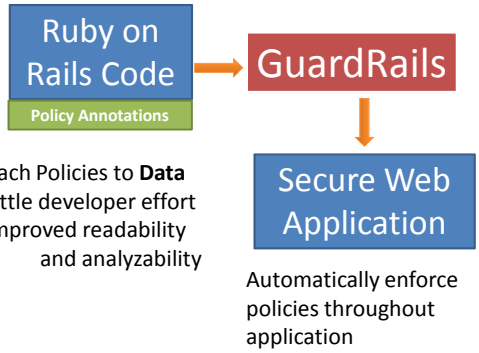
(Example from Redmine project management tool)

Input Validation

"User: " + user_name + ""

My user_name is "<script language='javascript'>doEvil();</script>"

(Cross-site scripting)



Attach Policies to **Data**
Little developer effort
Improved readability and analyzability

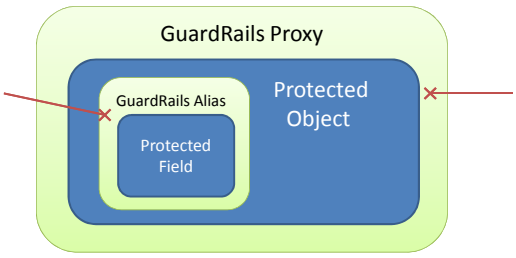
Automatically enforce policies throughout application

Example Policies

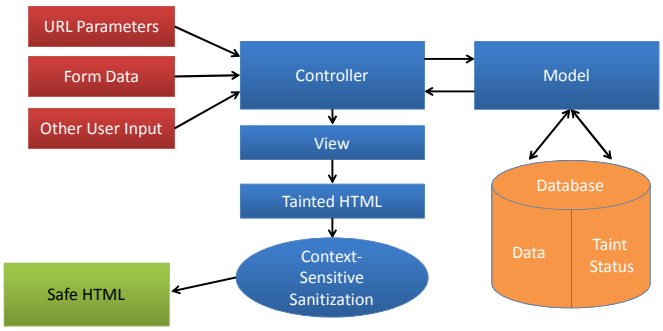
Annotation	Meaning
@delete, :admin, :to login	Only administrators can delete this object
@edit, *pswrd*, self.id == user.id, :to login	Only the user may change that user's password
@create, User, log_create; true	Whenever a User object is created, write to log

Policies are attached to classes or individual fields.
Can perform arbitrary checking and actions based on read, edit, append, create, destroy events.

Enforcing Policies



Taint Tracking



"**foo**" + "bar" → "**foo**bar"

Possible Projects

Automating Annotations

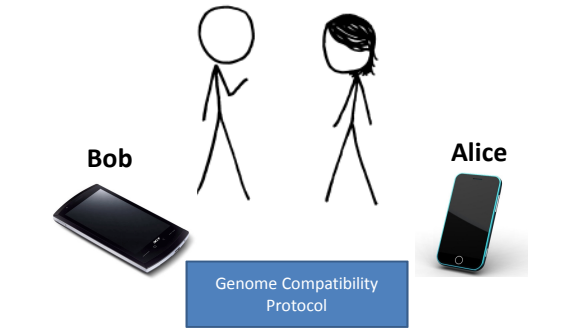
Client/Server Side Integration

Evaluation

Secure Computation in the Real(ish) World

Yan Huang (CS PhD)
Yikan Chen (CpE PhD)
Jerry Ye (BSCS 3)
Samee Zahur (CS PhD)

"Genetic Dating"



WARNING! Don't Reproduce

WARNING! Don't Reproduce

TheScientist News Current Issue Archive Sur

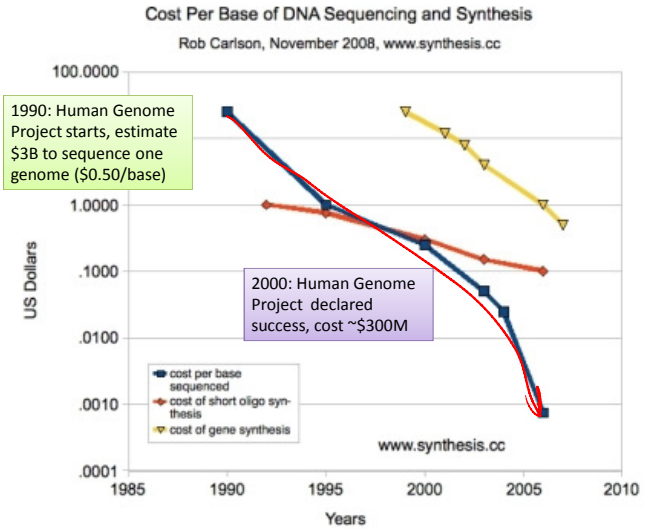
SHARE

2 comments
Comment on this news story

By Kerry Grens

Forget mistletoe - what about DNA?

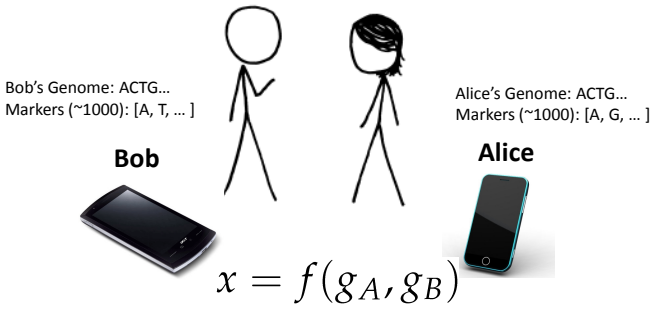
A new dating service matches singles using major histocompatibility complex genes



Year	reference	Technology	Sample	Average Reported Coverage depth (fold)	Reported sequencing consumables cost	Estimated cost per 40-fold coverage
	S4	Sanger (ABI)	JCV	7	$10,000,000	$57,000,000
	S5	Roche(454)	JDW	7	$1,000,000	$5,700,000
	S6	Illumina	NA18507	30	$250,000	$330,000
	S7	Helicos	SRQ	28	$48,000	$69,000
2009	this work	this work	NA07022	87	$8,005	$3,700
2009	this work	this work	NA19240	63	$3,451	$2,200
2009	this work	this work	NA20431	45	$1,726	$1,500

Human Genome Sequencing Using Unchained Base Reads on Self-Assembling DNA Nanoarrays. Radoje Drmanac, Andrew B. Sparks, Matthew J. Callow, Aaron L. Halpern, Norman L. Burns, Bahram G. Kermani, Paolo Carnevali, Igor Nazarenko, Geoffrey B. Nilsen, George Yeung, Fredrik Dahl, Andres Fernandez, Bryan Staker, Krishna P. Pant, Jonathan Baccash, Adam P. Borcherding, Anushka Brownley, Ryan Cedeno, Linsu Chen, Dan Chernikoff, Alex Cheung, Razvan Chirita, Benjamin Curson, Jessica C. Ebert, Coleen R. Hacker, Robert Hartlage, Brian Hauser, Steve Huang, Yuan Jiang, Vitali Karpinchyk, Mark Koenig, Calvin Kong, Tom Landers, Catherine Le, Jia Liu, Celeste E. McBride, Matt Morenzoni, Robert E. Morey, Karl Mutch, Helena Perazich, Kimberly Perry, Brock A. Peters, Joe Peterson, Charit L. Pethiyagoda, Kaliprasad Pothuraju, Claudia Richter, Abraham M. Rosenbaum, Shaunak Roy, Jay Shafto, Uladzislau Sharanhovich, Karen W. Shannon, Conrad G. Sheppy, Michel Sun, Joseph V. Thakuria, Anne Tran, Dylan Vu, Alexander Wait Zaranek, Xiaodi Wu, Snezana Drmanac, Arnold R. Oliphant, William C. Banyai, Bruce Martin, Dennis G. Ballinger, George M. Church, Clifford A. Reid. ***Science*, January 2010.**

Secure Two-Party Computation



Can Alice and Bob compute a function of their private data, without exposing anything about their data (other than the result)?

Secure Function Evaluation

Alice (circuit generator) **Bob (circuit evaluator)**

Picks $a \in \{0,1\}^s$ Agree on $f(a,b) \to x$ Picks $b \in \{0,1\}^t$

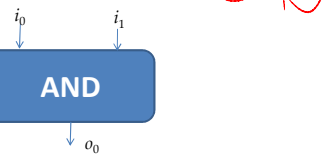
Garbled Circuit Protocol

Outputs $f(a,b)$ without revealing a to Bob or b to Alice.

Andrew Yao, 1982/1986

Computing with Lookup Tables

Input 0	Input 1	Output
0	0	0
0	1	0
1	0	0
1	1	1



Computing with Garbled Tables

Input 0	Input 1	Output
a_0	b_0	
a_0	b_1	
a_1	b_0	
a_1	b_1	

Computing with Garbled Tables

Input 0	Input 1	Output
a_0	b_0	$Enc_{a0,b0}(o_0)$
a_0	b_1	$Enc_{a0,b1}(o_0)$
a_1	b_0	$Enc_{a1,b0}(o_0)$
a_1	b_1	$Enc_{a1,b1}(o_1)$

Garbled Circuit Protocol

Alice (circuit generator) **Bob (circuit evaluator)**

Creates random keys: $a_0, a_1, b_0, b_1, o_0, o_1$

$E_{a_0,b_0}(o_0)$
$E_{a_1,b_1}(o_1)$
$E_{a_1,b_0}(o_0)$
$E_{a_0,b_1}(o_0)$

Sends a_i to Bob based on her input value a_0

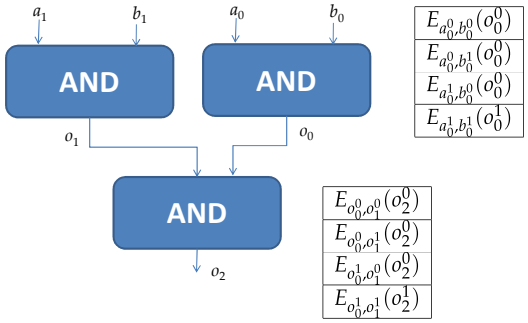
How does the Bob learn his own input wires?

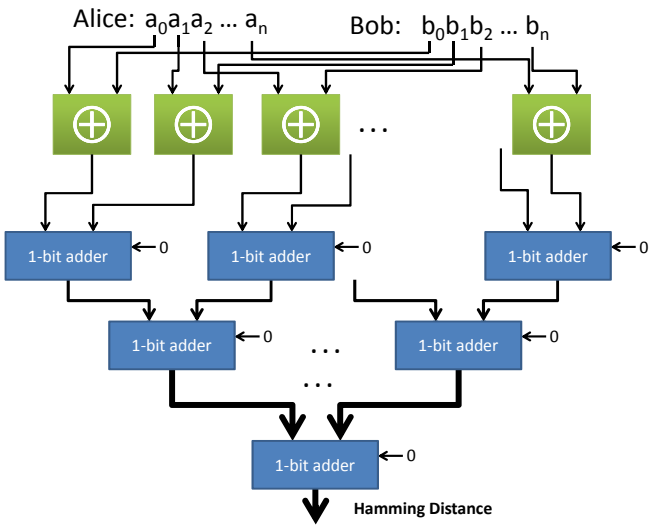
Primitive: **Oblivious Transfer**

Oblivious: Alice doesn't learn which secret Bob obtains
Transfer: Bob learns one of Alice's secrets

Rabin, 1981; Even, Goldreich, and Lempel, 1985; many subsequent papers

Chaining Garbled Circuits





Building Secure Computing Systems

We can do ***any*** computation privately this way!

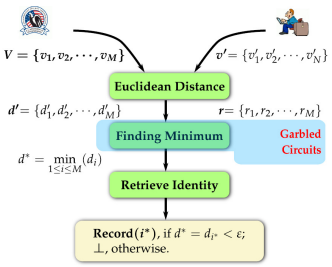
Cost metric very different from normal circuits

- Generating/evaluating each gate requires several encryption operations
- Can only execute each gate **once**
- **XOR** is free (and **NOT**) is nearly free

Framework for Efficiently Executing Circuits

- Pipeline generation and evaluation

Possible Projects



Design and implement a secure computation

- Fingerprint matching
- Genome analysis
- Image recognition
- Auctions

Improve garbled circuit evaluation

- Multi-core, GPU

Stronger Adversary Model