

CUTS: Coordinating User and Technical Security



Cyber Security Division 2012 Principal Investigators' Meeting

10/11/12

**Jim Blythe
Computer Scientist
USC Information Sciences Institute
blythe@isi.edu
310 448 8251**

CUTS Team

- Indiana University
 - Prof Jean Camp
 - Greg Norcie
 - Vaibhav Garg
 - Developer
 - Video Team
- USC/Information Sciences Institute
 - John Wroclawski
 - Jim Blythe
 - Intelligent Interaction Designer

TTA3: Usable Security

People are involved in most security decisions today.

Effective support for users can strengthen the link.

Intuitive, effective, timely security interactions.

“Unfortunately today, user involvement appears to be required too often and usually in terms that non-technical users have difficulty understanding, ..”

CUTS Technical Approach

CUTS will model the user and risk context to reason about the situation and communicate effectively

1. Track context to help identify problems and guide communication
2. Decision-theoretic approach to when and how much to communicate
3. Tailor risk communication with mental models
4. Coordinate response through automation

Example: falsified web certificates

Detection improved by context

- Potentially untrustworthy certificates found through machine learning approach
- Off-the-shelf learning combines context with observable world features and individual histories
 - age, blacklist, object of trust, ..
 - banking context – FDIC list

How to help the user make a good decision?



Secure Connection Failed

i.broke.the.internet.and.all.i.got.was.this.t-shirt.phreedom.org uses an invalid security certificate.

The certificate is not trusted because the issuer certificate has expired. The certificate expired on 9/1/2004 6:00 PM.

(Error code: sec_error_expired_issuer_certificate)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#)



How to help the user make a good decision



Secure Connection Failed

i.broke.the.internet.and.all.i.got.was.this.t-shirt.com uses an invalid security certificate.

The certificate is not trusted because the issuer certificate has expired. The certificate expired on 11/7/2004 6:00 PM.

(Error code: sec_error_expired_issuer_certificate)

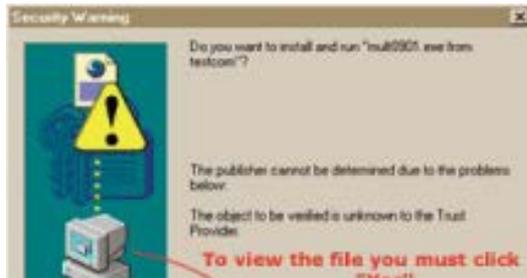
- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#)

At the wrong level



How to help the user make a good decision



Secure Connection Failed

i.broke.the.internet.com (img.godaddy.com) has a security certificate.

The certificate is not trusted because the issuer's certificate has expired. The certificate expired on 9/1/2006 6:00:00 PM.

(Error code: sec_err_cert_expired_issuer_certificate)

This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.

If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#)

At the wrong level, too frequent, not timely

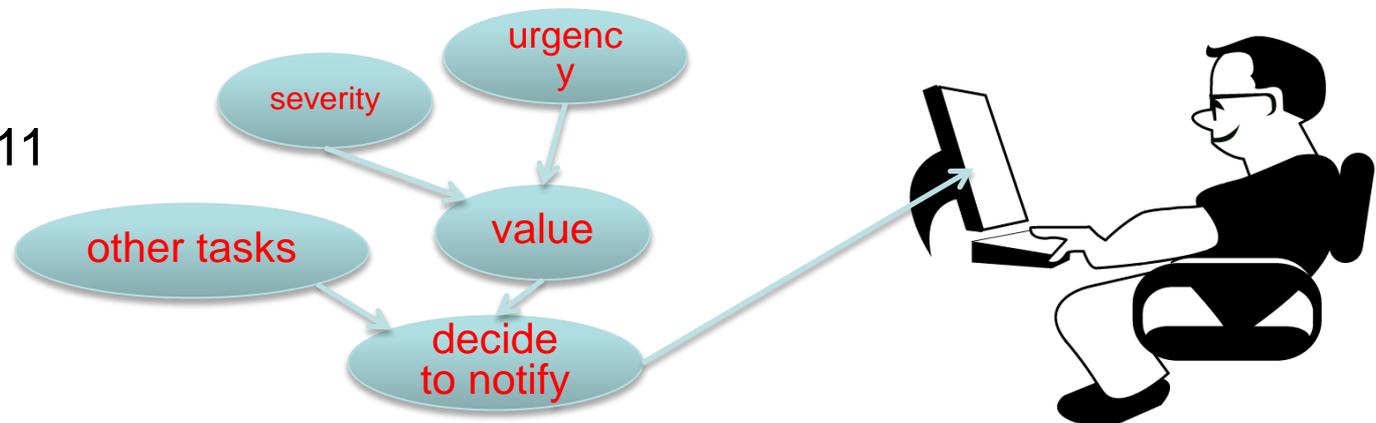


Intelligent communication

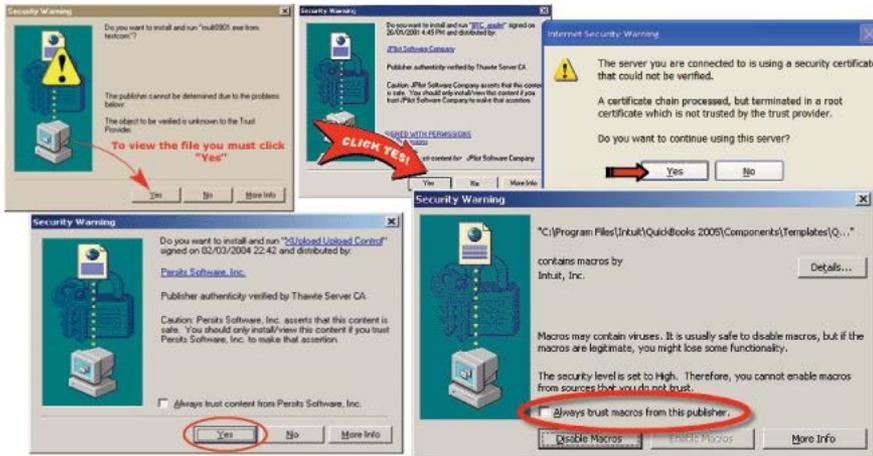
Don't warn too often. Pick moment so risk is in context.

- Probabilistic model of user's current task and distraction cost
 - includes security knowledge and decision biases
- Estimate expected value of communication:
 - Time-dependent expected value of advice vs distraction cost

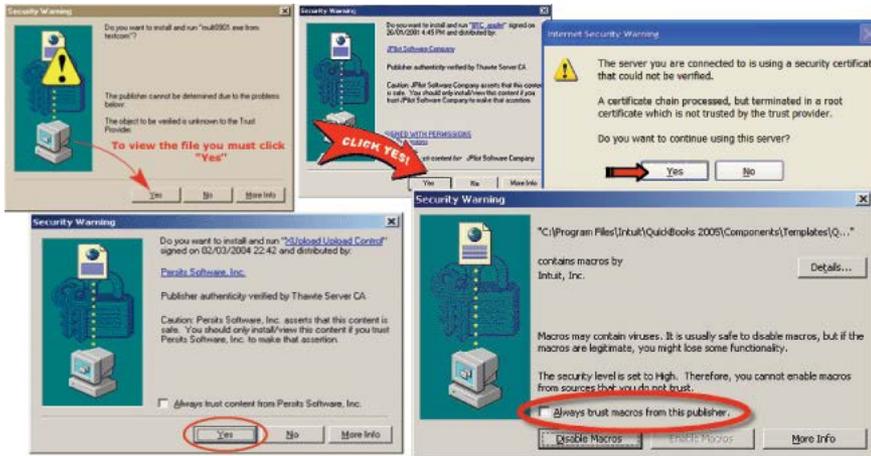
Blythe et al. 11



Communicate Risk



Communicate Risk

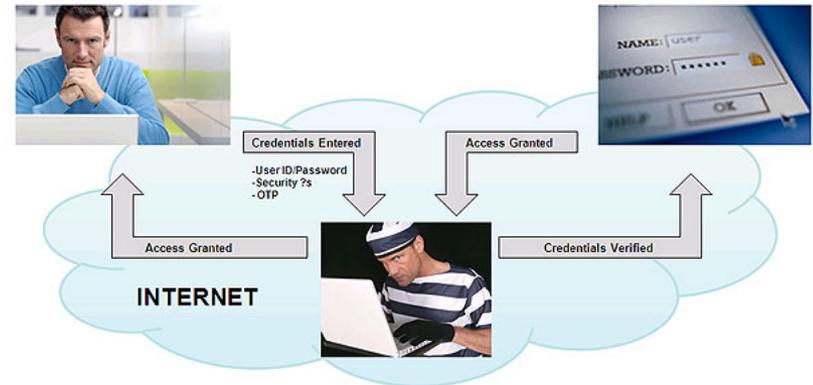


FreakingNews.com



Risk communication and mental models

- People reason *analogically* about security
- Design warnings and remedies to use common *mental models*



Camp 09
Blythe & Camp 12

Presenting responses at a higher level

- Possible actions in the same narrative
- Tailor security configurations to contexts, e.g. banking, browsing, working from home, ...
- Coordinate responses at higher level, e.g. “keep this message on the porch”.



= macros off,
scripting off,
halt background downloads
low warning threshold

Deliverables

Operational prototype including:

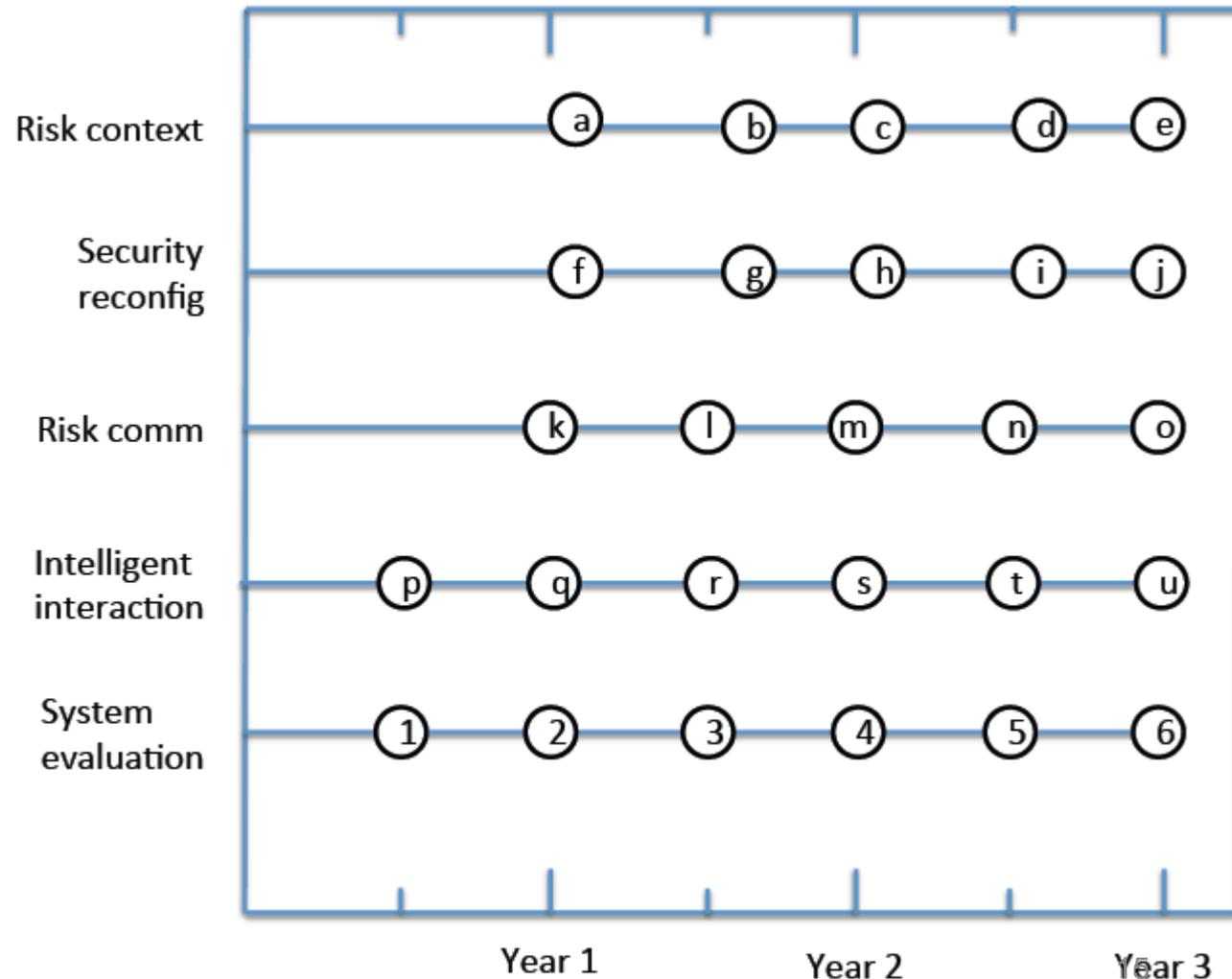
- Context detection
- Network state identification
- Intelligent interaction
- Automated setting adjustment
- Data isolation

Videos, stills & wizards for targeted interaction

Monthly, quarterly and annual reports

Schedule

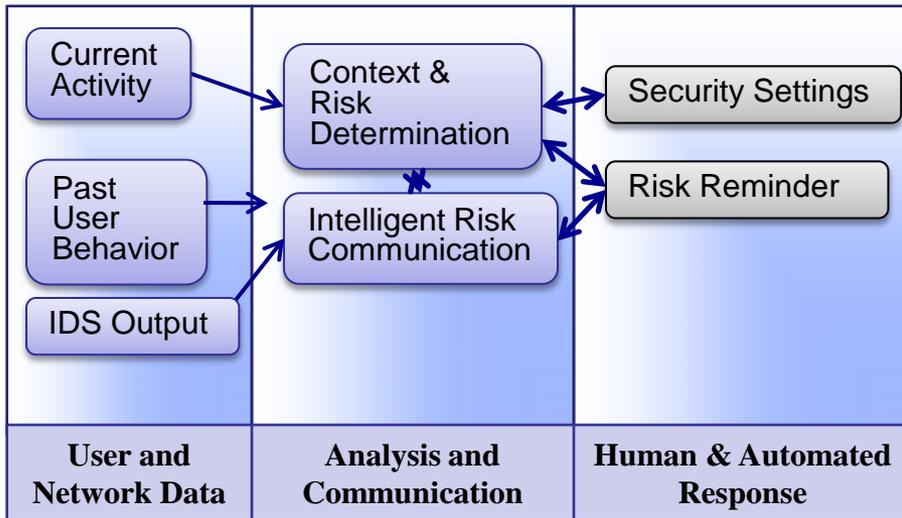
- Continual evaluation with users
- Develop components in year 1
- Initial prototype, year 2
- Full prototype in year 3



Transition plan

- Will identify advisory board and partners for open-source diffusion
 - Current partners are ISOC & Mozilla
- Year 2 prototype available through DETER and Google Open Source
- Identify diffusion partners and detailed commercialization plan by year 3

Quad chart



Operational Capability

1. Significant decrease efficacy of human engineering attacks, protect critical user data in cases of other attacks.
2. Improve security behaviors and simultaneously decreasing the time spent managing security settings by implementing intuitive warnings with context-specific defaults.
3. The proposed prototype is client-centric software, with an open source diffusion model.
4. The prototype would meet the goals of TTA #3 by intelligently automating the resolution of many security related issues that today require excessive user interaction, and engaging the user intuitively rather than mechanically when interaction is required.

Proposed Technical Approach

1. The proposal meets the goals of TTA #3 through 1) broadening, hardening, and expanding an innovative user-centered security system to an operational prototype; 2) develop timely effective communications that obsolete current pop-up dialogues.
2. Expanding, hardening, and testing (technical and human subjects) prototype into fully functional prototype.
3. The current technology is proof of concept context recognition and tested, proven but single instantiation of intuitive interactions.
4. Implemented operating proof of concept, developed multimedia warnings, integrated warning into browsing, evaluated user response in laboratory and in-situ.
5. Related efforts are research (not development) funded by NSF and maintenance of previous code base.

Schedule, Cost, Deliverables, & Contact Info

- Milestones are completion of risk context analysis, security reconfiguration, risk communication, intelligent interaction, and system evaluation. Over 30 months the development, testing, expansion and hardening of the current proof-of-concept system. Testing and development are an iterative cycle throughout these months. This is a 6 months further development option for an optimization for a specified institution, including demonstrations.
- Deliverables: Fully functional translucent security prototype
- Corporate Information: Offeror POC: Steven A. Martin, Associate Vice President for Research Administration, PO Box 1847, Office of Research Administration, Indiana U., Bloomington, IN 47402