Threat Modeling for Game Developers

Stephen Beeman
Proprietor, Gizmocracy
stephen.beeman@gizmocracy.com

Game Developers Conference® Online 2011
October 10-13, 2011 | Austin, TX
www.GDCOnline.com

Not My First Rodeo

- Programming games since 1978 (TRS-80, represent!)
- Wrote my first LAN game in 1984
- Wrote my first online game for Microsoft in 1996
- Director of Online Technology for Origin
- Lead program manager for server security and infrastructure, MSN Games (Windows/C#)
- System architect for Superhero Squad Online (Linux/ Python & Java)

The Three Questions

1. "What's the problem?"
2. "What will it take to make it go away?"
3. "What happens if I just ignore you?"

Definition

- Threat modeling is a process by which a system is methodically analyzed to find, evaluate and mitigate vulnerabilities.

- Threat modeling looks at your system the way an attacker does.

Definition

- A process by which a system is methodically analyzed to find, evaluate and mitigate vulnerabilities.

Definition

- A process by which a system is methodically analyzed to find, evaluate and mitigate vulnerabilities.

Definition

- A process by which a system is methodically analyzed to find, evaluate and mitigate vulnerabilities.

Definition

- A process by which a system is methodically analyzed to find, evaluate and mitigate vulnerabilities.

Definition

- A process by which a system is methodically analyzed to find, evaluate and mitigate vulnerabilities.

Definition

- A process by which a system is methodically analyzed to find, evaluate and mitigate vulnerabilities.

The Process

a) Enumerate threats
b) Construct threat trees
c) List vulnerabilities
d) Calculate risks
e) Take action
f) Repeat

Enumerate threats

- Threats = exploits x assets

Exploit taxonomy: STRIDE

- Pretending to be another user: spoofing
- Modifying data outside of normal usage: tampering
- Erasing the history of an action: repudiation
- Reading data outside of normal usage: information disclosure
- Preventing the system from functioning: denial of service
- Getting permission to perform forbidden actions: elevation of privilege

Example: Auth Cookie

- Spoofing: Create a valid cookie for a real user, or for a fake one
- Tampering: Modify part of a valid cookie
- Repudiation: ...
- Information disclosure: Grab another user's cookie
- Denial of service: ...
- Elevation of privilege: Add permissions tokens to a cookie

Example: Auth Cookie

- Spoofing: Create a valid cookie for a real user, or for a fake one
- Tampering: Modify part of a valid cookie
- Repudiation: ...
- Information disclosure: Grab another user's cookie
- Denial of service: ...
- Elevation of privilege: Add permissions tokens to a cookie

Attacker could create a fake auth cookie [S]

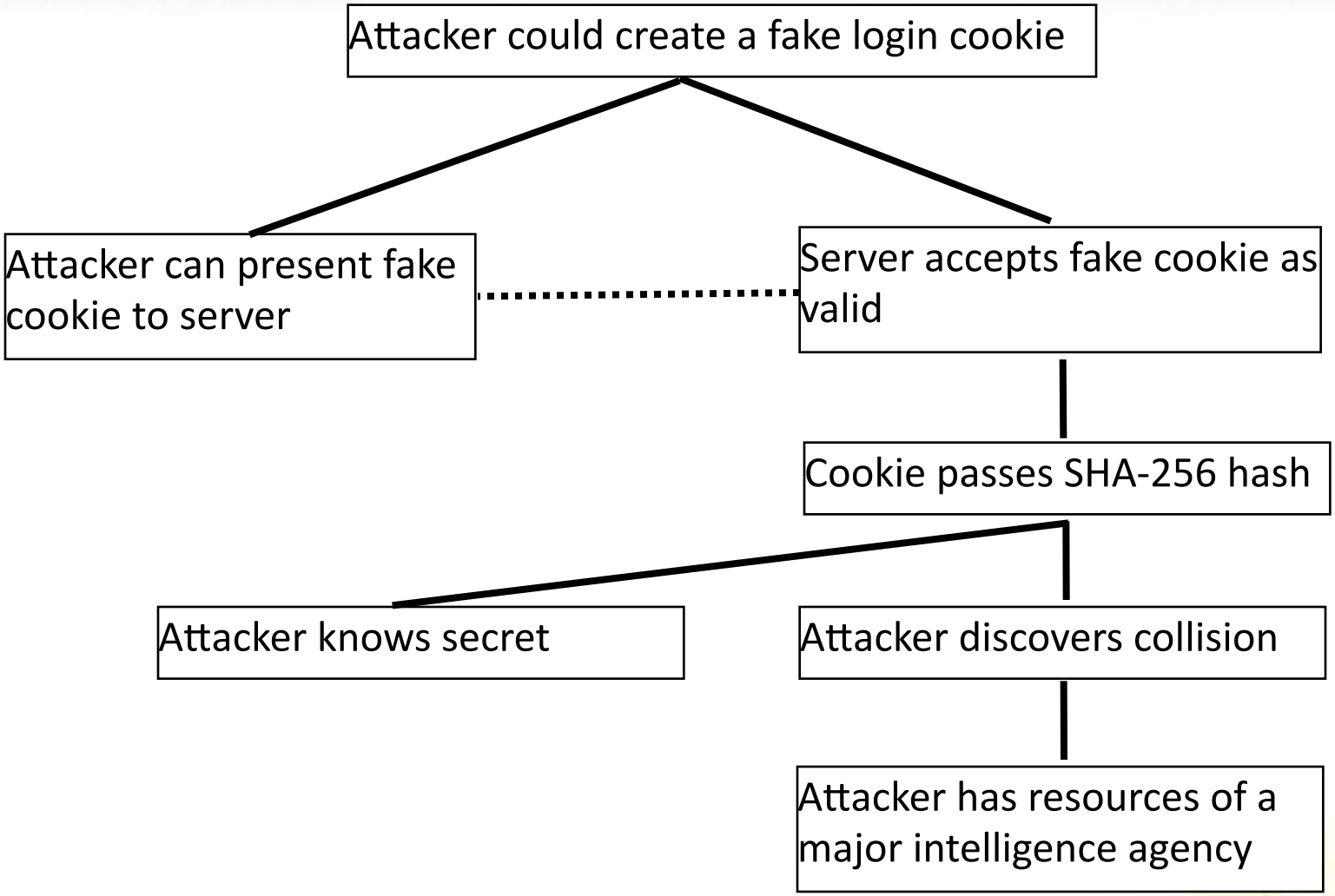
Attacker could modify a valid auth cookie [T]

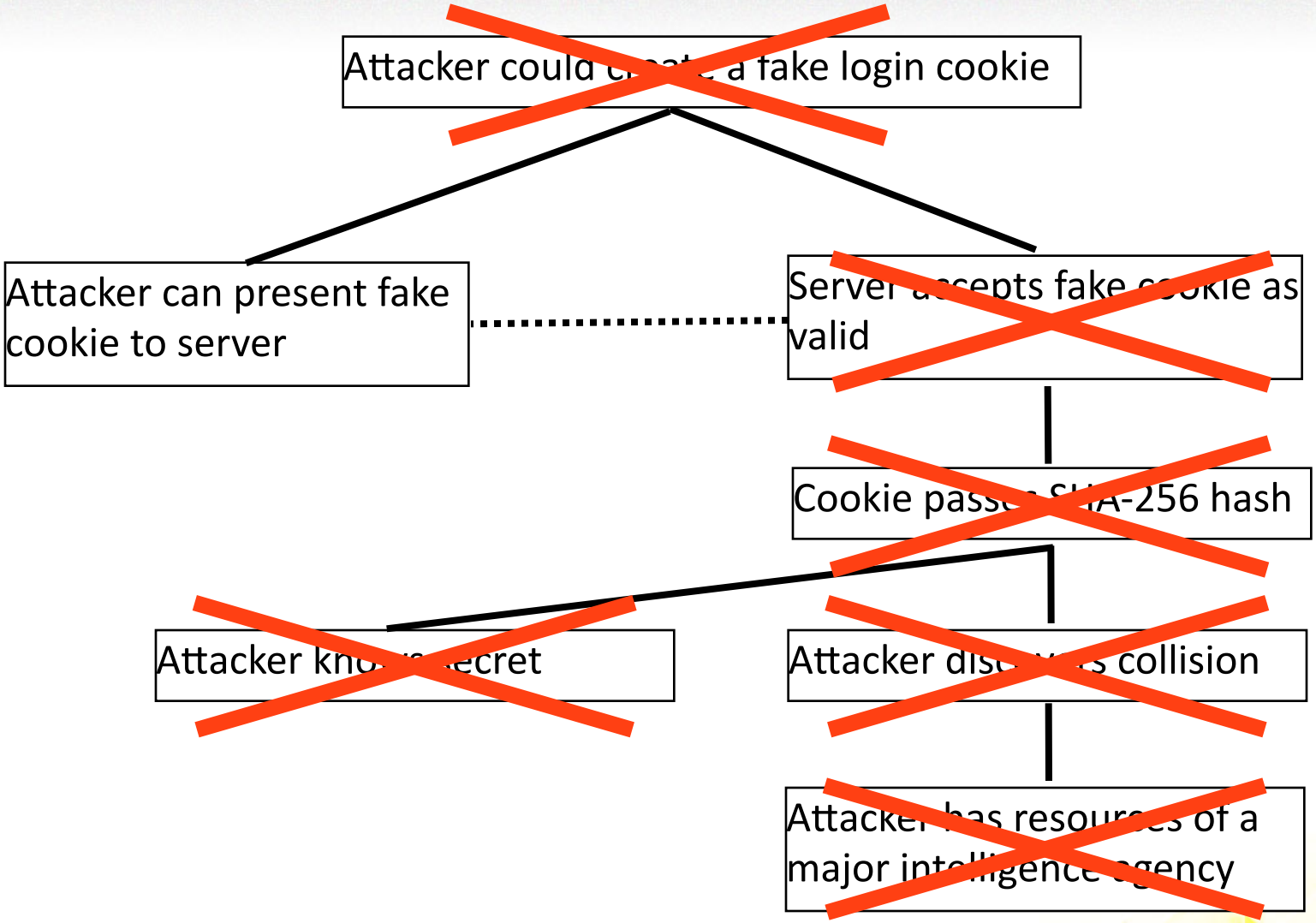
Attacker could gain access to another user's valid auth cookie [I]

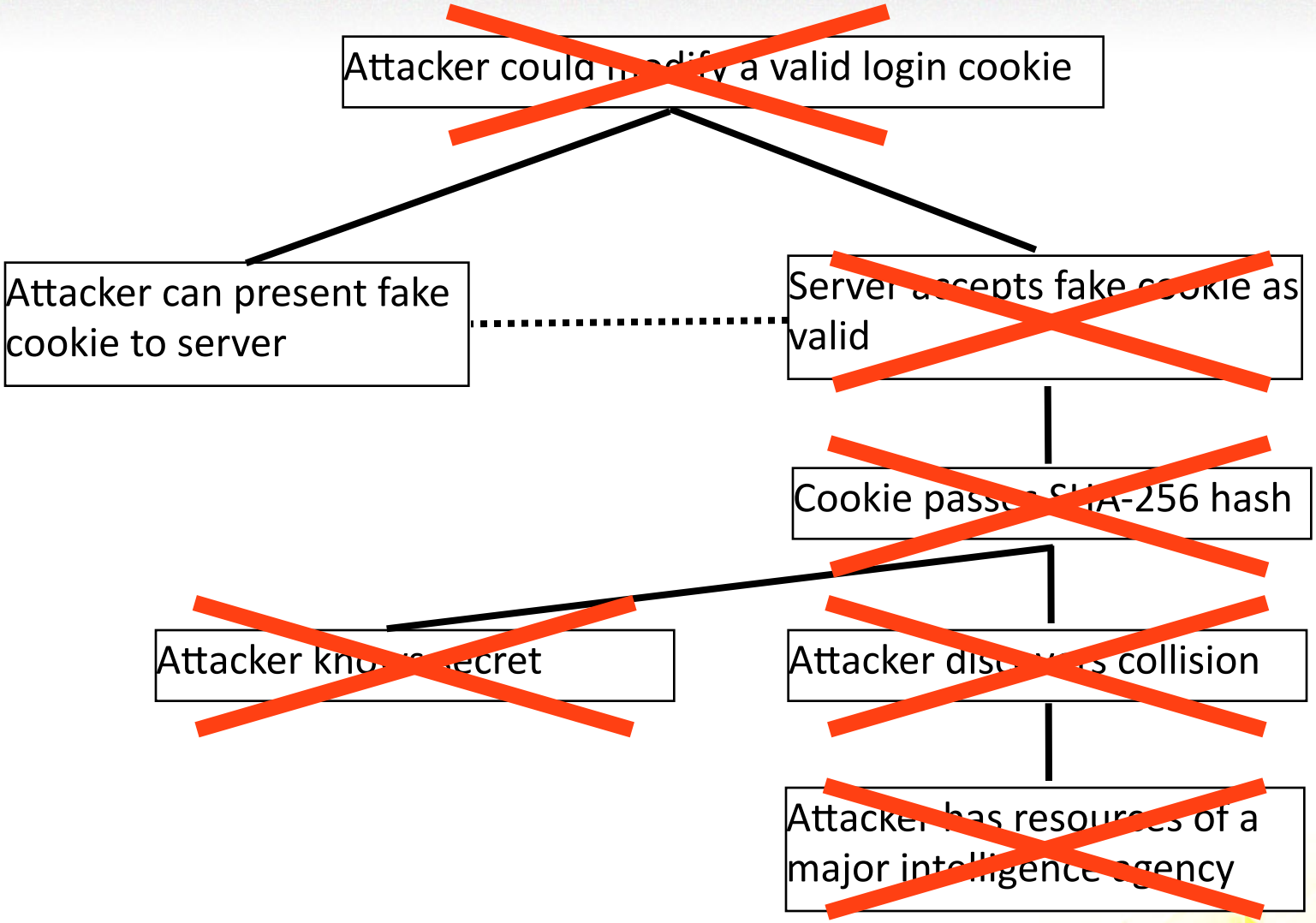
Construct threat trees

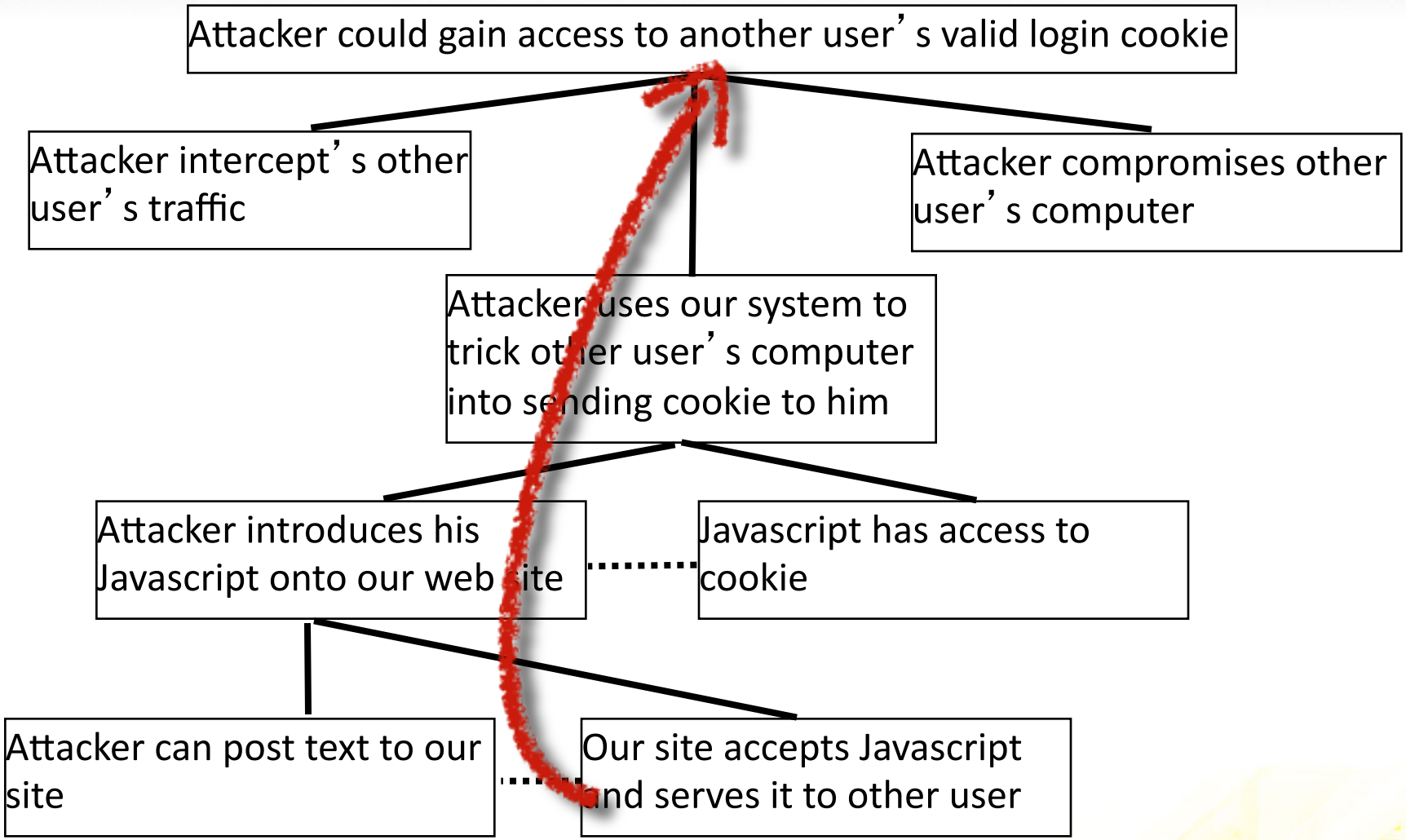
- A threat tree is a diagram that describes what must be true for an attacker to carry out the specified threat.

- The topmost node is the threat itself. Each child is a condition that, if true, means the threat can be carried out. Each child in turn has its own children.


Attacker could create a fake login cookie
Attacker can present fake cookie to server
Server accepts fake cookie as valid
Cookie passes SHA-256 hash
Attacker knows secret
Attacker discovers collision
Attacker has resources of a major intelligence agency


Attacker could create a fake login cookie
Attacker can present fake cookie to server
Server accepts fake cookie as valid
Cookie passes SHA-256 hash
Attacker knows secret
Attacker discovers collision
Attacker has resources of a major intelligence agency


Attacker can present fake cookie to server
valid
Attacker knows secret
Attacker discovers collision
major intelligence agency


Attacker could gain access to another user's valid login cookie
Attacker intercept's other user's traffic
Attacker compromises other user's computer
Attacker uses our system to trick other user's computer into sending cookie to him
Attacker introduces his Javascript onto our web site
Javascript has access to cookie
Attacker can post text to our site
Our site accepts Javascript and serves it to other user

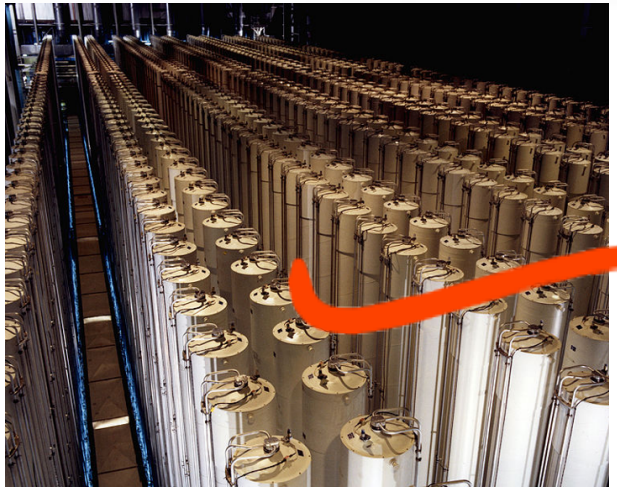
Calculate risks

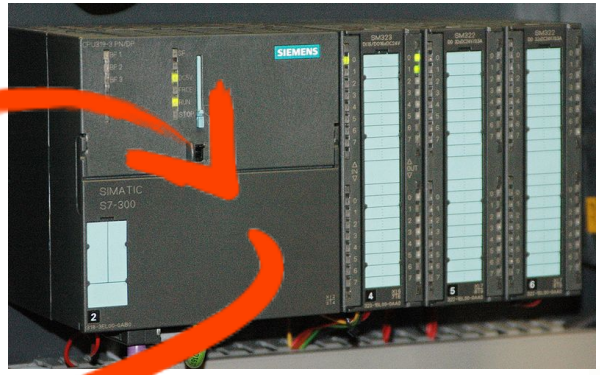
- A vulnerability is a threat whose threat tree contains one or more valid paths from bottom to top.

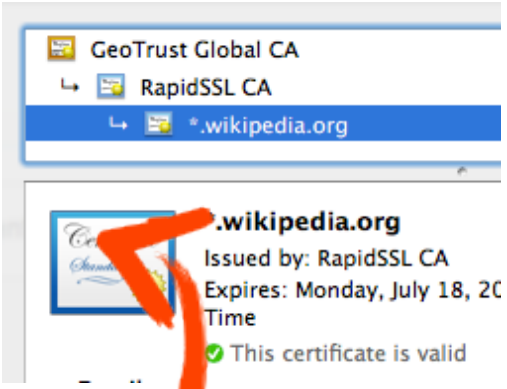
That doesn't mean it needs to be mitigated!

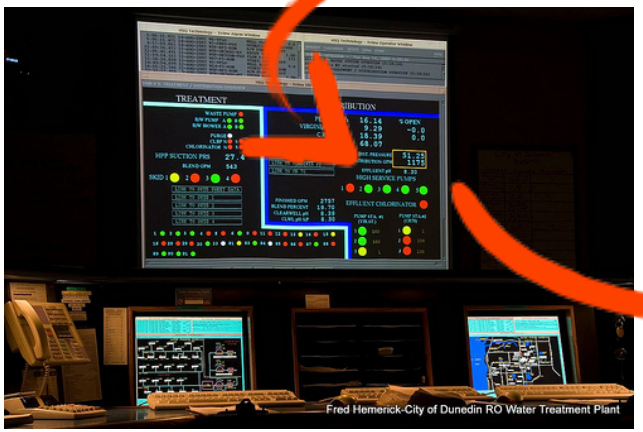
- Seriously:

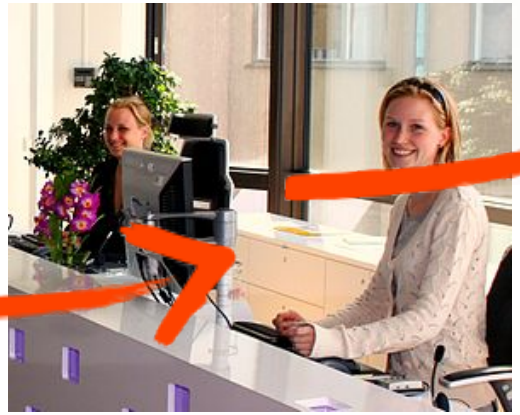
- There is no such thing as perfect security.



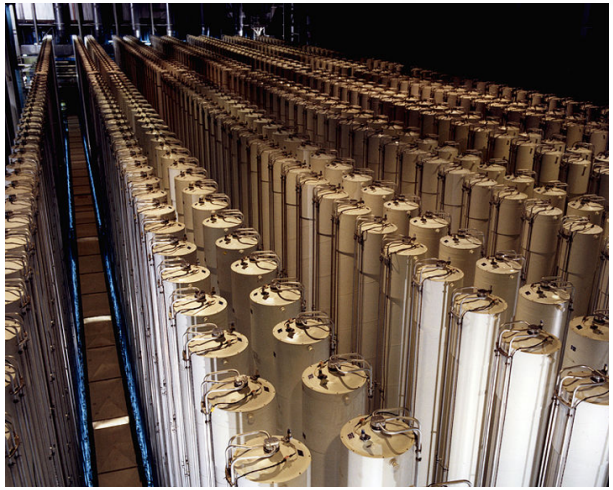

SIEMENS
SIMATIC
S7-300


GeoTrust Global CA
RapidSSL CA
*.wikipedia.org
.wikipedia.org
Issued by: RapidSSL CA
Expires: Monday, July 18, 20
Time
This certificate is valid

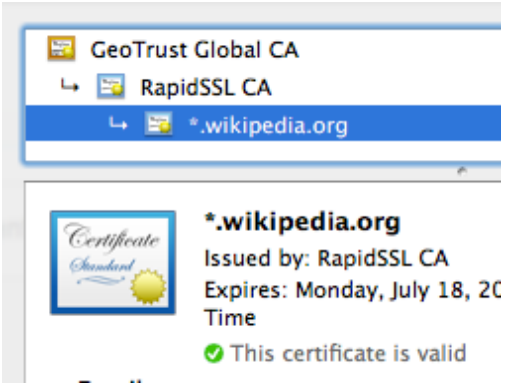

TREATMENT
Fred Hemerick-City of Dunedin RO Water Treatment Plant




cruzer
micro
4 GB




SIEMENS
SIMATIC
S7-300


GeoTrust Global CA
RapidSSL CA
*.wikipedia.org
*.wikipedia.org
Issued by: RapidSSL CA
Expires: Monday, July 18, 20
Time
This certificate is valid


TREATMENT
DISTRIBUTION
Fred Hemerick-City of Dunedin RO Water Treatment Plant


cruzer
micro
4 GB

Risk = likelihood x cost

- The fundamental question about any vulnerability is "What happens if we just ignore it?"
- The risk posed by an event is its likelihood multiplied by the cost that event would impose if it took place.
-

Risk rating: REAL

- Reward: What's the attacker get out of it?
- Effort: How little does the attacker have to work?
- Audience: How many people will be affected?
- Level of skill: How many attackers have the skill required to carry out the attack?

- Assign each a value from 1 to 10, multiply them all together and move the decimal two to the left, for a value from 0.01 to 100.0.

Attacker could gain access to another user's valid login cookie

- Reward: 10.
- Effort: 8.
- Audience: 10.
- Level of skill: 8.

- Total risk: 64.0.

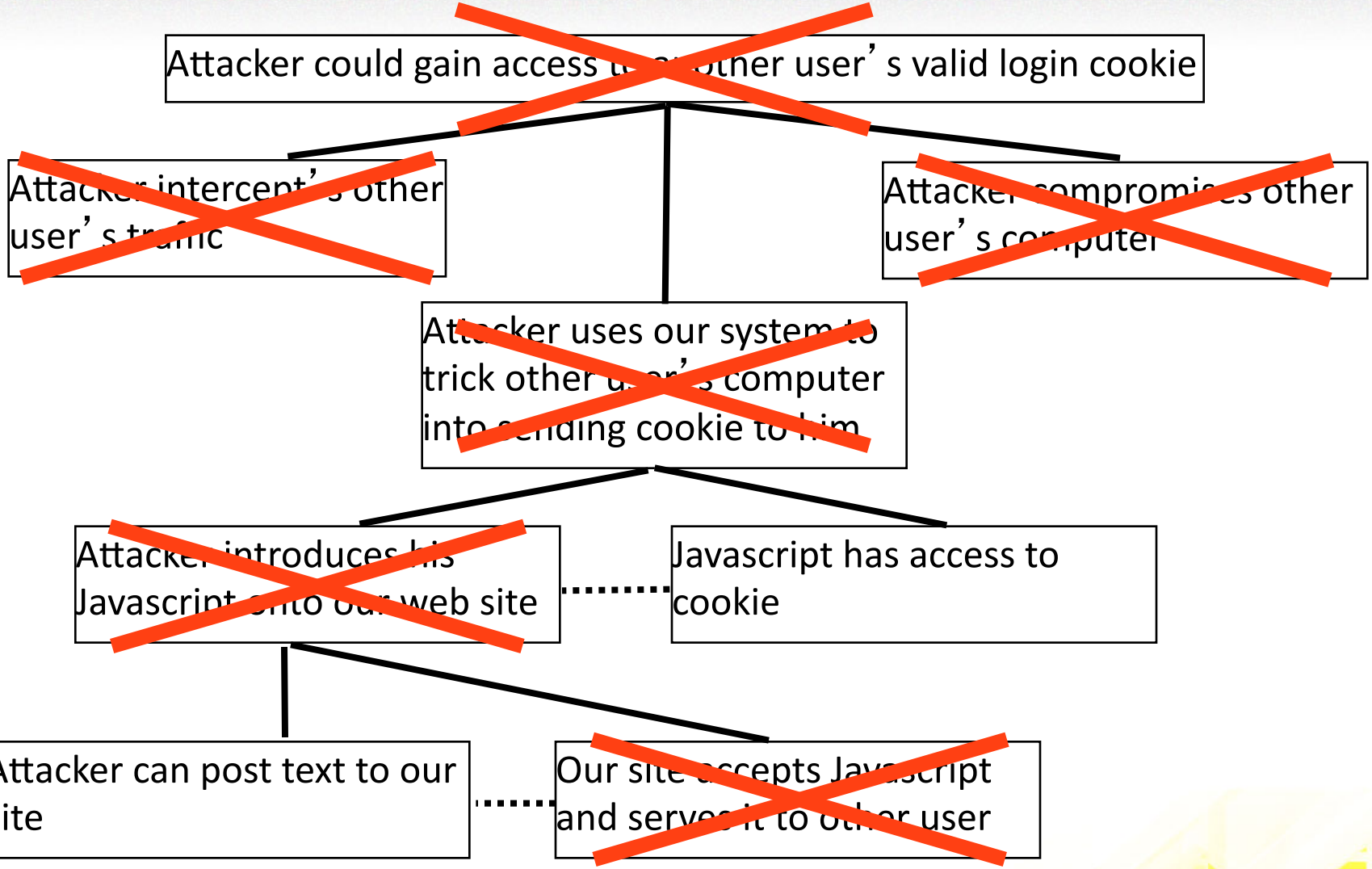
Take action

- Set your security bar, the risk rating above which you will act on a vulnerability.
- Enter the vulnerabilities above that bar into your bug database. The ones below that bar go into your backlog.
- Act on the vulnerabilities that cross your bar.

Mitigating vulnerabilities

- Two choices:

1. Change the circumstances so that paths through the threat tree are closed off
2. Change the risk variables so that the vulnerability falls below the bar


Attacker could gain access to another user's valid login cookie
Attacker intercepts other user's traffic
Attacker compromises other user's computer
Attacker uses our system to trick other user's computer into sending cookie to him
Attacker introduces his Javascript onto our web site
Javascript has access to cookie
Attacker can post text to our site
Our site accepts Javascript and serves it to other user

Change the risk

- This is perfectly legitimate!

- Reduce the reward!
- Increase the effort!
- Limit the audience!
- Raise the skill level!

Reduce the risk enough, and you can call it a "real" mitigation

Security through design

Security through education

Security through business development

Repeat!

a) Review and update threats
b) Review and update threat trees
c) Review and update mitigations
d) Identify new vulnerabilities
e) Recalculate risks and adjust security bar
f) Address more vulnerabilities

Responsibilities

- Programming: Review threat model for validity and currency; create mitigations
- Production: Manage process and documentation; review risks and adjust security bar
- Design: Create mitigations
- Test: Verify mitigations; maintain security bug list.
- Operations: Review threat model for validity and currency; create mitigations.
  - Ops can and should be doing their own threat modeling of data-center and OS-level security.

Responsibilities

- Customer service: Review risk ratings; prepare for known vulnerabilities; identify new vulnerabilities in the wild.
- Business development: Create mitigations; review and adjust risk ratings; prepare for known vulnerabilities.
- Community management: Create mitigations; review risk ratings; prepare for known vulnerabilities; identify new vulnerabilities in the wild.

What We've Learned

a) Enumerate threats
b) Construct threat trees
c) List vulnerabilities
d) Calculate risks
e) Take action
f) Repeat

Next Steps

Threat Modeling
Frank Swiderski and Window Snyder
Microsoft Press

http://www.microsoft.com/security/sdl/

Other search terms: “attack modeling”, “risk modeling”

stephen.beeman@gmail.com

Q & A