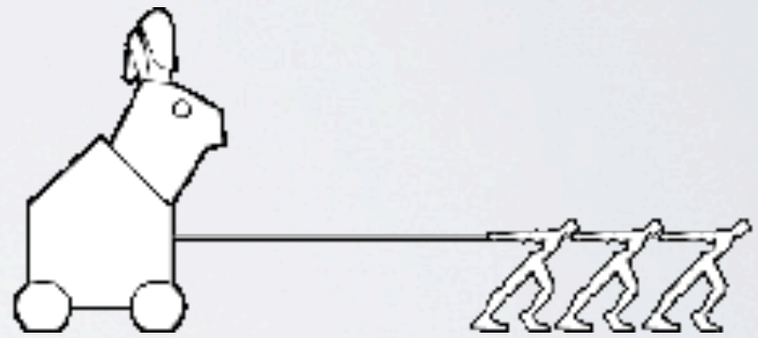
THE RATIONAL REJECTION OF SECURITY ADVICE

Cormac Herley

NSPW

The New Security Paradigms Workshop (NSPW) is an annual, small invitation-only workshop for researchers in information security and related disciplines. NSPW's focus is on work that challenges the dominant approaches and perspectives in computer security.



STATE OF THE UNION

- unpatched Windows will be compromised within 12 minutes
- security advice is complex and growing
- benefit is invisible and largely speculative
- users will choose the weakest they can get away with
- user education has failed

3 VIEWPOINTS

1. users are hopelessly lazy
2. security tasks must be made more usable
3. rejection of security advice is entirely rational

EXAMPLE 1: PASSWORDS

1. Choose a long password.
2. Compose it using mixed case, digits and special characters.
3. Don't use dictionary words.
4. Don't write it down.
5. Don't share it with anyone.
6. Change it often.
7. Don't re-use passwords across sites.

ACTUAL BENEFITS

- there is no scientific data on the nature of password attacks
- Paypal: fraud ratio 0.49% = $8.8 million
- with 70 million active users, security advice should cost no more than $8.8/70 = $0.1257 annually
- that's one minute of minimum wage time per year
- banks even reimburse user losses

EXAMPLE 2: PHISHING

- it is very hard for users to check URLs for phishing
  - www.paypa l .com, www.paypal.com.evil.com, …
- US annual phishing loss is estimated at $60 million
- given 180 million US online population, this amounts to $0.33 per user, or 2.6 minutes per year at minimum wage
- any advice that requires more time is economically more harmful than phishing itself

EXAMPLE 3: CERTIFICATES

- 100% of certificate errors are false positives
- bad sites simply do not use SSL
- checking certificates offers only abstract protection
- the effort is real, the harm only theoretical

IMPLICATIONS

- there is no hard data on the risks
- worst case harm is not actual harm
- user effort is not free
- designing security advice is not an unconstrained optimization

DISCUSSION

- questioning the overall method
  - Can all losses be expressed financially? What about privacy?
  - Is this an argument against any security?
  - Why do people use insurances?
- questioning the actual arguments
  - Are security and convenience really adversaries?