Understanding and Altering Users’ Motivation to Follow Computer Security Advice
A RATIONAL DECISION MODEL APPROACH
Mohammad Maifi Khan
February 9, 2017 | Noon | Maurer Law 335 (lunch provided)

Usable security researchers have long seen interest in what users do to keep their devices and data safe and how that compares to recommendations. Additionally, experts have long debated and studied the psychological underpinnings and motivations for users to do what they do, especially when such behavior is seen as risky, at least to experts. This talk will survey our work on users’ motivation behind their online decisions, and will discuss the key gaps in perception between those who follow common security advice (i.e., update software, use a password manager, use 2FA, change passwords) and those who do not. Finally, findings from one of our recent studies that investigated the effectiveness of informational videos that are designed to provide information about two-step verification (i.e., 2FA) and improve users’ adoption rate of 2FA will be presented.

Mohammad Maifi Khan is an Assistant Professor in the Computer Science and Engineering Department in the School of Engineering at University of Connecticut. He received his B.Sc. Engineering degree in Computer Science and Engineering from BUET, Bangladesh, and MS and PhD degree in Computer Science from University of Illinois, Urbana-Champaign. His research revolves around different aspects of system reliability and usability such as performance modeling and troubleshooting of large scale systems, mitigating the effect of system failures on system usability, and improving user’s compliance rate towards recommended online behavior. His published work spans a diverse range of fields, including usable authentication, risk communication, distributed protocol design and troubleshooting, and wireless sensor systems.
Assignment 1 is due! Assignment 2 is out and is due in two weeks!

(2017-02-14)

(Please get started early!!)
Recall: Stream cipher

Idea: Replace the truly random pad used by the OTP encryption scheme with a pseudorandom pad

- Let $G: \{0,1\}^* \rightarrow \{0,1\}^*$ be a PRG with expansion factor $\ell$
- Plaintexts / ciphertexts are $\ell(n)$-bit strings; key is an $n$-bit string
  - $\text{Gen}(1^n)$ outputs a uniform random key $k \in \{0,1\}^n$
  - $\text{Enc}_k(m)$ computes XOR of $m$ and $G(k)$; that is, $c := m \oplus G(k)$
  - $\text{Dec}_k(m)$ computes XOR of $c$ and $G(k)$; that is, $m := c \oplus G(k)$
Indistinguishability against eavesdroppers

\[ \text{Adv}_{\text{onetime}}(A) := \left| \Pr[b = b'] - \frac{1}{2} \right| \]

Challenger (C)

- \( k \leftarrow \text{Gen}(1^n) \)
- \( b \in_R \{0, 1\} \)
- \( c \leftarrow \text{Enc}_k(m_b) \)

Attacker (A)

- \( m_0, m_1 \in \{0, 1\}^n \)

One-time indistinguishability game
Indistinguishability against eavesdroppers

**Defn:** An encryption scheme $(\text{Gen}, \text{Enc}, \text{Dec})$ has indistinguishable encryptions in the presence of an eavesdropper if, for every PPT algorithm $A$, there exists a negligible function $\varepsilon: \mathbb{N} \to \mathbb{R}^+$ such that

$$\text{Adv}_{\text{one-time}}(A) \leq \varepsilon(n)$$
Pseudorandom generators (PRGs)

• Informally, a PRG is a deterministic algorithm that, on input a truly random $n$-bit seed, outputs a “random looking” $\ell(n)$-bit stream for some $\ell(n) > n$

Q: How do we formalize the notion of a string being “random looking”?
A: Very carefully...
Game 0:

Challenger (C)

1^n

k ∈ \{0, 1\}^n

r := G(k)

r ∈ \{0, 1\}^\ell(n)

Attacker (A)

1^n

b'

Game 1:

Challenger (C)

1^n

r ∈ \{0, 1\}^\ell(n)

Attacker (A)

1^n

b'

Def^n: \text{Adv}^{PRG}(A) := \frac{1}{2} - \Pr[b' = 0 \text{ in game 0 or } b' = 1 \text{ in game 1}]
Distinguishing distributions

- What tactics might the distinguisher employ?
  - Output 0 if hamming weight of $r$ is "implausibly" large or small
  - Output 0 if substring "00" occurs implausibly often in $r$
  - Output 0 if $r$ contains a run of more than $2 \log |r|$ consecutive 0s
  - And so on and so forth...

Q: Which set of tests is the correct one to consider?
- Fact: Given any fixed set of tests, it is easy to construct $G$ that passes them all, yet is easily distinguished using some other test
Fixed-expansion PRG

Defn: Let $G: \{0,1\}^* \rightarrow \{0,1\}^*$ and let $\ell: \mathbb{N} \rightarrow \mathbb{N}$ be a pair of deterministic functions such that, $\forall n \in \mathbb{N}$ and $\forall k \in \{0,1\}^n$, $G(k) \in \{0,1\}^{\ell(n)}$. Then $G$ is a fixed-expansion pseudorandom generator (PRG) if:

1. $\forall n \in \mathbb{N}$, $\ell(n) > n$ (\(\ell\) is called the expansion factor of $G$)
2. For every PPT algorithm $A$, there is a negligible function $\varepsilon: \mathbb{N} \rightarrow \mathbb{R}^+$ such that $\text{Adv}^{\text{PRG}}(A) \leq \varepsilon(n)$
Computational indistinguishability

**Defn:** Two probability ensembles \( \{X_n\}_{n \in \mathbb{N}} \) and \( \{Y_n\}_{n \in \mathbb{N}} \) are (computationally) indistinguishable if, for every PPT algorithm \( A \), there exists a negligible function \( \varepsilon: \mathbb{N} \rightarrow \mathbb{R}^+ \) such that

\[
|\Pr[A(X_n)=1] - \Pr[A(Y_n)=1]| \leq \varepsilon(n)
\]
Fixed-expansion PRG (alt. defⁿ)

Defⁿ: Let $G: \{0,1\}^* \rightarrow \{0,1\}^*$ and $\ell: \mathbb{N} \rightarrow \mathbb{N}$ be a pair of deterministic functions such that, $\forall n \in \mathbb{N}$ and $\forall k \in \{0,1\}^n$, $G(k) \in \{0,1\}^{\ell(n)}$. Then $G$ is a fixed-expansion pseudorandom generator (PRG) if:

1. $\forall n \in \mathbb{N}$, $\ell(n) > n$ (\(\ell\) is called the expansion factor of $G$)
2. The distribution ensembles
   $$\{G(U_n)\}_{n \in \mathbb{N}} \text{ and } \{U_{\ell(n)}\}_{n \in \mathbb{N}}$$
   are computationally indistinguishable, where for each $n \in \mathbb{N}$, $U_n$ denotes the uniform distribution.
An example of a PRG?

Example: Define $G : \{0,1\}^* \rightarrow \{0,1\}^*$ s.t. $G(k) = k \mathbin{\|} (k_1 \oplus k_2 \oplus \cdots \oplus k_{|k|})$

where $k_i$ denotes the $i$th bit of $k$

- Expansion factor: $\ell(s) = s + 1$
- Is $G$ a PRG? No!

Q: How do we prove that $G$ is not a PRG?

A: Construct an efficient distinguisher!

- $D(r)$ output 1 if and only if the XOR of all bits in $r$ is 0
- $\text{Adv}^{\text{PRG}}(D) = |P^r - 1/2| = 1/2$ (which is not negligible!)
That’s all for today, folks!