

# OVERCOMING SECURITY AND PRIVACY RISKS IN THE HOME

TADAYOSHI KOHNO  
(UNIVERSITY OF WASHINGTON)

# WHAT DEVICES IN THE HOME?

---



Make existing computational devices / services better?

# WHAT DEVICES IN THE HOME?



Newly computational; new features

# WHAT DEVICES IN THE HOME?



**POTENTIAL SECURITY AND  
PRIVACY CONCERNS?**



Newly computational; new features

# WHAT DEVICES IN THE HOME?

WHAT IS THE LIKELIHOOD THAT NEW PRODUCTS WILL BE “SECURE” AND “PRIVATE”?

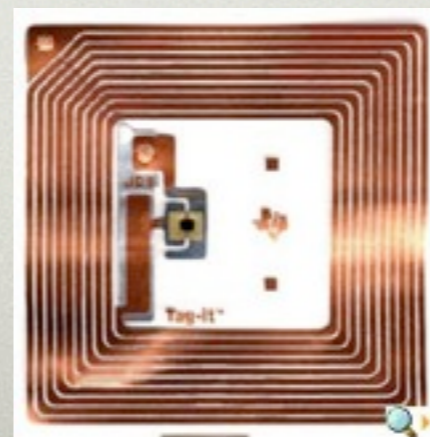
Newly computational; new features




# EXAMPLE “OPPORTUNITIES”

---

- Cat (RFIDs) infected with computer virus (<http://www.rfidvirus.org/>)
- Nike+iPod (UW)
- Implantable Defibrillators (UW+UMass+BIDMC/Harvard)



# WHAT DEVICES IN THE HOME?

A collage of various smart home devices and furniture. On the left, a stainless steel double oven is shown. In the center, a bed with a wooden headboard and a red sofa are visible. On the right, a pair of purple and green headphones is shown. At the bottom left, a white toilet is depicted. In the bottom center, a smart speaker with a textured top is shown. At the bottom right, a dog is wearing a harness. A large yellow box with a red border is overlaid in the center, containing the text.

**BUT WOULD ANYONE  
EXPLOIT THESE  
VULNERABILITIES?**

Newly computational; new features

# NOVEMBER 2007

## PRESS RELEASE

Receive press releases from coping-with-epilepsy.com: [By Email](#)

RSS Feeds: [XML](#) [+ MY Yahoo!](#)

### Hooligans Attack Epilepsy Patients During Epilepsy Awareness Month

*Hooligans attack epilepsy support forum in an attempt to induce seizures amongst the members.*

Houston, TX, November 19, 2007 --(PR.com)-- Internet

"I was able to trace back the source of the attack to a handful of sites where the perpetrators were instigating the event," said Bernard Ertl, CWE Administrator. **"It was just a bunch of very immature people delighting in their attempts to cause people misery.** Attacking sites is just a way to pass time for them. Unfortunately, this time they tried to hurt people. Seizures are not a laughing matter. A member of CWE passed away just two weeks ago from a seizure. SUDEP (Sudden Unexplained Death in Epilepsy) is a very real and serious concern."

serious concern."

"Since the attack, CWE has implemented modifications to discourage future attempts at malfeasance," remarked Ertl. "This was the first time CWE has been targeted in this manner. I guess in a way it's a testament to the growing popularity of the site. We're working to ensure that there will never be a repeat performance."

Ironically, the attack occurred during November, which is National Epilepsy Awareness Month.

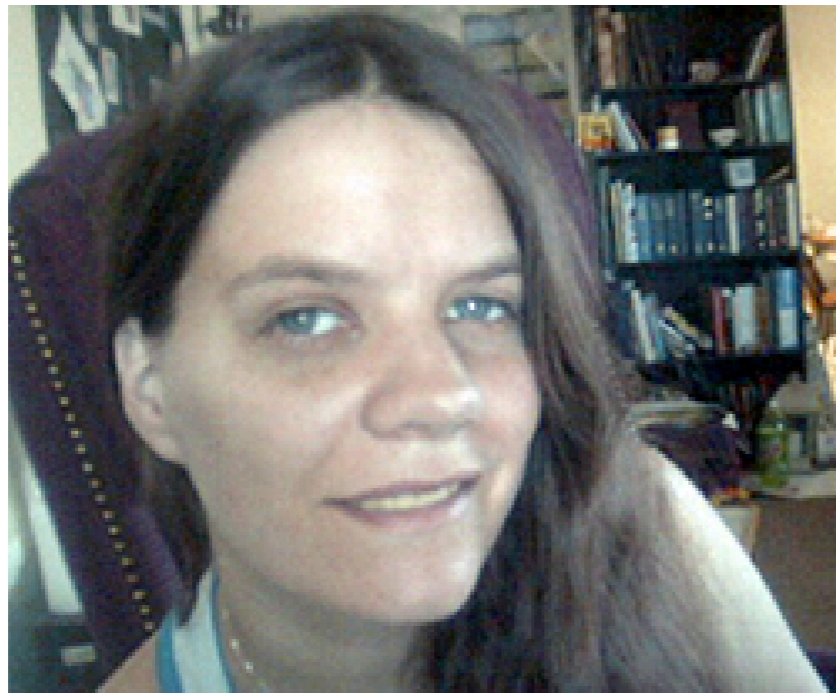
#### About CWE

Coping With Epilepsy is a peer support forum for people living with epilepsy. It boasts a world-wide membership including medical professionals.

# AGAIN IN MARCH 2008

## Hackers Assault Epilepsy Patients via Computer

By Kevin Poulsen  03.28.08 | 8:00 PM



Internet griefers descended on an epilepsy support message board last weekend and used JavaScript code and flashing computer animation to trigger migraine headaches and seizures in some users.

The nonprofit [Epilepsy Foundation](#), which runs the forum, briefly closed the site Sunday to purge the offending messages and to boost security.

"We are seeing people affected," says Ken Lowenberg, senior director of web and print publishing at the Epilepsy Foundation. "It's fortunately only a handful. It's possible

**"This was clearly an act of vandalism with the intent to harm people, and we shut the attack down immediately,"** said Eric R. Hargis, president and CEO of the Epilepsy Foundation

injecting JavaScript into some posts that redirected users' browsers to a page with a more complex image designed to trigger seizures in both photosensitive and pattern-sensitive epileptics.

# WHY ARE NEW DEVICES SO OFTEN INSECURE?

Numbers here are estimates; for new devices (not desktop computers and applications)

- 85% { 1. Oversight: Designers didn't consider security and privacy
- 2. Choice: Designers chose to ignore security and privacy
- 10% { 3. Definitions: What does security mean?
- 4. Mistakes: "Easy" solutions, flawed implementation (includes usability issues)
- 5% { 5. Technical challenges: Fundamental technical obstacles

Need to overcome all 5. Need to overcome 1-4 first

# TECHNICAL CHALLENGES

---

- Definitions
- Component diversity
- Evolving components
- Limited interfaces
- Physical interaction
- Remote access
- Who's the "user"?
- Who's the "administrator"?

# ADDRESSING OVERSIGHT AND CHOICE

---

If we believe that security and privacy are important...

- Increase consumer demand
  - Media?
  - Public service education?
  - Consumer Reports?
- Top down:
  - Legislation
    - Toy safety; FDA
  - Liability
- Computer science and engineering education



# WHY ARE NEW DEVICES SO OFTEN INSECURE?

---

- 85% { 1. Oversight: Designers didn't consider security and privacy
- 2. Choice: Designers chose to ignore security and privacy
- 10% { 3. Definitions: What does security mean?
- 4. Mistakes: "Easy" solutions, flawed implementation (includes usability issues)
- 5% { 5. Technical challenges: Fundamental technical obstacles

Need to overcome all 5. Need to overcome 1-4 first