Who am I?

@SecBarbie
Credentials?
SPACE CAMP
(1986)
“Life imitates art far more than art imitates Life.”
-Oscar Wilde
SPACE CAMP
(1986)
We need to work harder and faster to fight for the users!
Won't that be grand?
Computers and the programs will start thinking and the people will stop.

- Dr. Walter Gibbs
SHALL WE PLAY A GAME?
WarGames (1983)

“I don’t believe any system is totally secure”
NATIONAL POLICY ON TELECOMMUNICATIONS
AND AUTOMATED INFORMATION SYSTEMS SECURITY (U)

Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The
D.A.R.Y.L.
(1985)
2010 – "Jackpotting" ATMs
Barnaby Jack
SNEAKERS
(1992)
February 16, 2016

A Message to Our Customers

The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand.

This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake.

Answers to your questions about privacy and security ›

The Need for Encryption

Smartphones, led by iPhone, have become an essential part of our lives. People use them to store an incredible amount of personal information, from our private conversations to our photos, our music, our
JURASSIC PARK
(1993)
JURASSIC PARK
(1993)
Why San Francisco's network admin went rogue

An inside source reveals details of missteps and misunderstandings in the curious case of Terry Childs, network kidnapper

Last Sunday, Terry Childs, a network administrator employed by the City of San Francisco, was arrested and taken into custody, charged with four counts of computer tampering. He remains in jail, held on $5 million bail. News reports have depicted a rogue admin taking a network hostage for reasons unknown, but new information from a source close to the situation presents a different picture.

In posts to my blog, I postulated about what might have occurred. Based on the small amount of public information, I guessed that the situation revolved around the network itself, not the data or the servers. A quote from a city official that Cisco was getting involved seemed to back that up, so I assumed that Childs must have locked down the routers and switches that form the FiberWAN network, and nobody but Childs knew the logins. If this were true, then regaining control over those network components would cause some service disruption, but would hardly constitute the "millions of dollars in damages" that city representatives feared.
HACKERS
(1995)
THE ITALIAN JOB
(2003)
Key signals targeted, officials say

Two accused of hacking into L.A.'s traffic light system plead not guilty. They allegedly chose intersections they knew would cause major jams.

**January 09, 2007 |** Sharon Bernstein and Andrew Blankstein | Times Staff Writers

Back in August, the union representing the city's traffic engineers vowed that on the day of their work action, "Los Angeles is not going to be a fun place to drive."

City officials took the threat seriously.

Fearful that the strikers could wreak havoc on the surface street system, they temporarily blocked all engineers from access to the computer that controls traffic signals.

But officials now allege that two engineers, Kartik Patel and Gabriel Murillo, figured out how to hack in anyway. With a few clicks on a laptop computer, the pair -- one a renowned traffic engineer profiled in the national media, the other a computer whiz who helped build the system -- allegedly tied up traffic at four intersections for several days.

Both men pleaded not guilty Monday morning to felony charges stemming from the case, and Murillo's lawyer said his client meant no harm when he signed on to the system that day.
What if?
GONE IN 60 SECONDS
(2000)
What do I need to know?

- Offline time
- Does it do notification
- How long does the notification take?
- Does it notify you if it comes back online?
- Any cached video
- Onboard video storage
- Wired network option
- Type of power (Battery vs. Wired)
- Addition Equipment needed for function?
- Other performance observations
How was it tested?

• 0:00 – Stopwatch starts
• 1:00 – Targeted De-authorization Begins
  • Every :30 Hand wave for motion recognition
• 11:00 – Targeted De-authorization Ends
• 16:00 – Test ends
The Setup

- **Timer**
- **Test Camera**
- iPad w/ Cam Apps on Separate Network
You get the idea,
Now what to do with the data?
Time to get some information
What about the keys?
Thieves using a $17 power amplifier to break into cars with remote keyless systems
Who cares!
SECURITY?

This is what an indoor security camera should be.
See your home 24/7.

Circle is the modern home security camera
For Your Business Security!

Meet Canary, the all-in-one home security system you control from your phone. It’s built to learn and sends

One security system. Endless possibilities.

100% Wire-free
Arlo Wire-Free cameras mean no cords, no outlets, and no limits on where your cameras can go or what they can watch

Smart Alerts
Arlo cameras detect motion and send you alerts instantly so you know when something unexpected happens.
“Security”
Not being sold as "Security"
Summary of Issues

We are not solving the most basic problems

And about that wireless CCTV

*Most* WiFi Security Cameras can get blasted offline and see/know nothing
How do we help?

We need to Fight For the Users!
MR. ROBOT
(TV - Present)
Citations

http://cogweb.ucla.edu/Abstracts/Wilde_1889.html
http://fas.org/irp/offdocs/nsdd145.htm
https://www.rand.org/content/dam/rand/pubs/papers/2005/P3544.pdf