cloakware™ by irdeto

THE SPREAD OF CYBERTHREATS

How Hackers Are Connecting with Your Organization

John O'Connor | Mark Hearn

"…A REFRIGERATOR IS A COMPUTER THAT KEEPS THINGS COLD…"

"As the chairman pointed out, there are now computers in everything. But I want to suggest another way of thinking about it in that EVERYTHING IS NOW A COMPUTER: This is not a phone. It's a computer that makes phone calls. A refrigerator is a computer that keeps things cold. ATM machine is a computer with money inside. Your car is not a mechanical device with a computer. It's a computer with four wheels and an engine… And this is the Internet of Things, and this is what caused the DDoS attack we're talking about."

– BRUCE SCHNEIER

speaking before members of US Congress (Nov. 2016)

cloakware™

HACKS DAMAGE BRAND, INTELLECTUAL PROPERTY, SAFETY AND COST $$$$

CONSIDER THE BALANCE OF THE DIFFERENT BUSINESSES

Security Spend

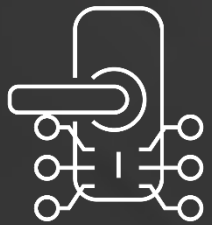
Hacker Profit

cloakware™

WHAT WAS THEIR THOUGHT PROCESS?

DEVELOPER

Do I have any code vulnerabilities in the lock tumbler?



SECURITY ARCHITECT

I need to have a strong lock on the front door, steel frame, locking windows and alarm system on all ground floor openings

HACKER

Who in the neighborhood has the nicest things AND is easiest to get into

cloakware™

WHAT DO HACKERS LOOK FOR?

YOUR DATA

Intellectual Property

Personal Information

$

THE PATH TO YOUR DATA

Break the crypto

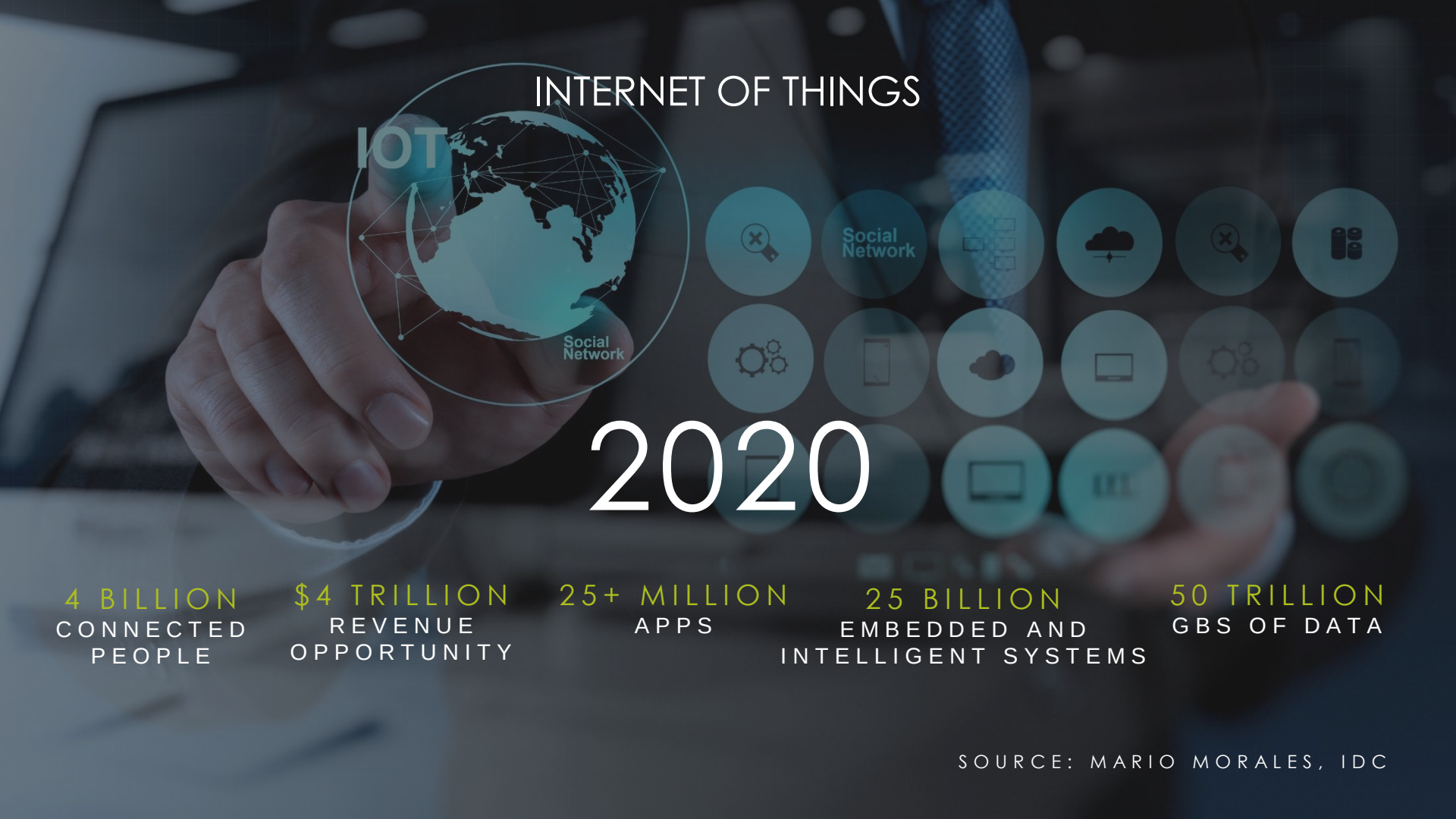
Look for patterns

PUT THE 2 TOGETHER

$$

Leverage

INTERNET OF THINGS



2020

4 BILLION
CONNECTED PEOPLE

$4 TRILLION
REVENUE OPPORTUNITY

25+ MILLION
APPS

25 BILLION
EMBEDDED AND INTELLIGENT SYSTEMS

50 TRILLION
GBS OF DATA

SOURCE: MARIO MORALES, IDC

AIRBORNE

4G

WIFI

BLUETOOTH

ZIGBEE

Z WAVE

PANDEMIC

pan·dem·ic

/panˈdemik/

adjective

1. (of a disease) prevalent over a whole country or the world.
   synonyms: widespread, prevalent, pervasive, rife, rampant
   "the disease is pandemic in Africa"

noun

1. an outbreak of a pandemic disease.

cloakware™

HACKER'S VIEW | NO PROTECTION

STRAIGHT PATH
CLEAR VISIBILITY

AN ATTACKER HAS THE ADVANTAGE

- Most people don't think maliciously.
- If you think something is a unique edge case, that's what the attacker will go after.
- You release your product. Attacker may not. Forensics of a hack can be difficult.
- Hacking is black magic to most people.

cloakware™

ANATOMY OF AN ATTACK

ATTACK SURFACE

The Device
(receives the most focus)

Smartphone app
(everyone has one)

Communications
(the bit that makes it connected)

The things the device connects to

Cloud (via the Internet)

PHASES OF AN ATTACK

Investigation

Leverage a weakness

Rinse and repeat

Create an attack

Scale the attack

$$$$

I SECURE MY COMMUNICATIONS, SO I KNOW THAT I CAN TRUST THE DATA I RECEIVE.

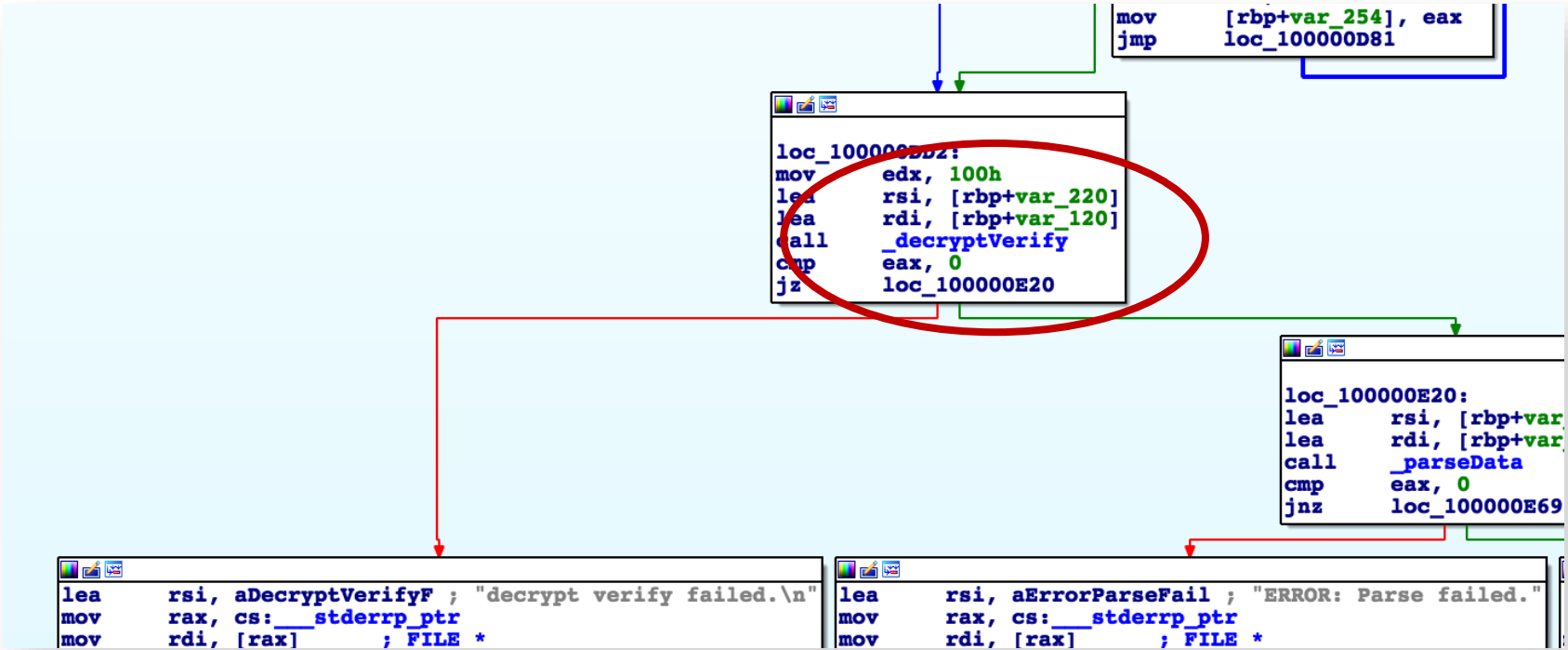
"MY DATA IS SAFE BECAUSE IT'S ENCRYPTED…"

BUT THE ATTACK IS DIFFERENT ON EXPOSED ENDPOINTS

- "Yes, brute forcing encryption is not feasible if proper key entropy is used."
- So, the attacker goal is to gain privileged access to an endpoint.
  - They try to "find the ladder".
- With endpoint access, attacker won't have to break the crypto. They wait for you to decrypt it, then attacker will take it.

REMEMBER, CODE IS READABLE

REVERSE ENGINEERING TO FIND DECRYPTED DATA

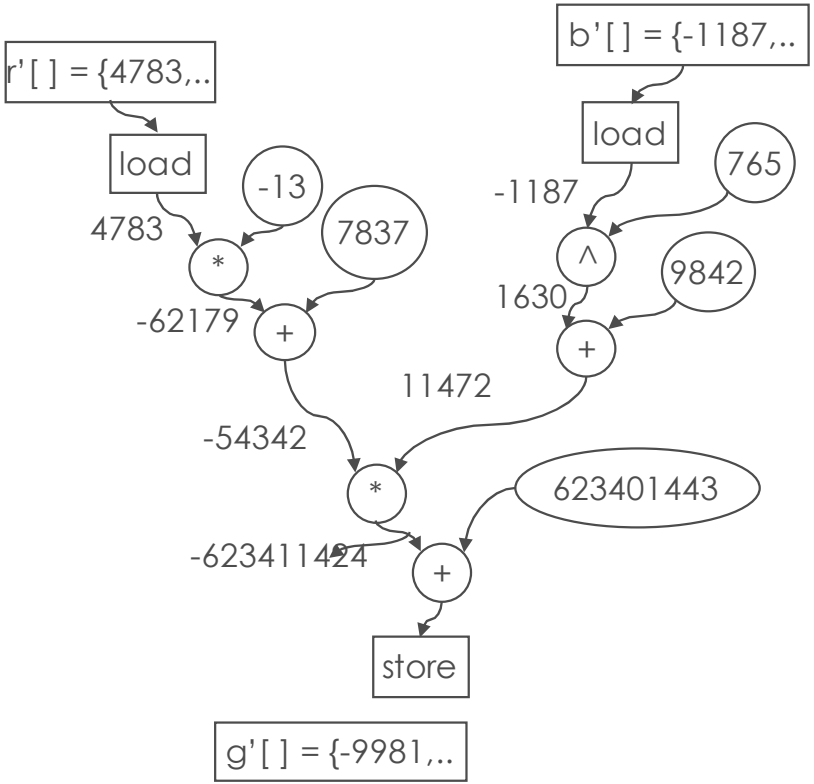


cloakware™

HACKER'S VIEW | ADVANCED PROTECTION

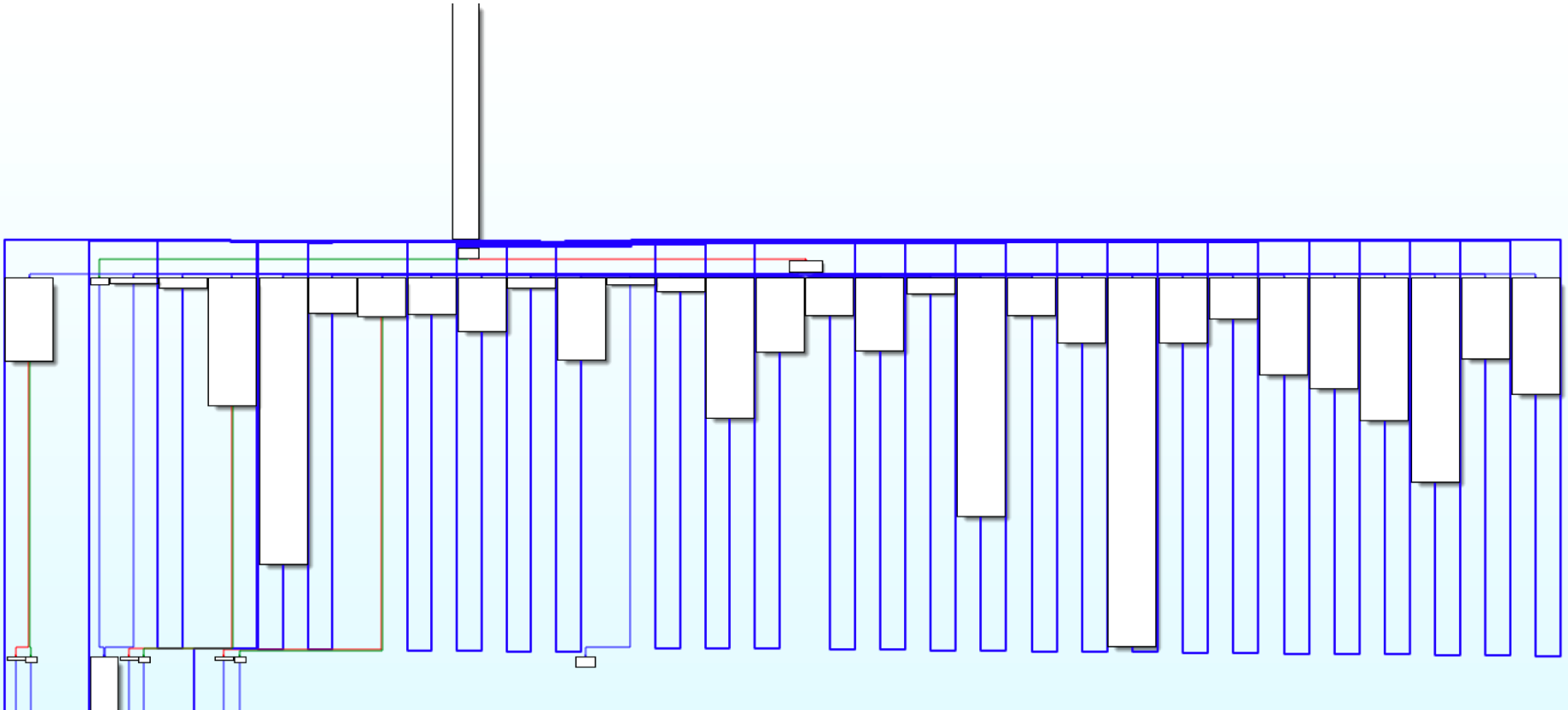
WHAT IF YOU COULD PROCESS YOUR DATA WITHOUT HAVING IT IN A CLEAR STATE?

TO COMPLEXITY



WHAT IF YOU COULD HIDE THE FLOW CHART IN YOUR CODE?

TO FLATTENED CODE



ONGOING SECURITY STRATGY = DEFENSE IN DEPTH

Technology	Prevent Analysis		Prevent Tampering		Foil Automated Attacks	Renew and Diversify
	Static	Dynamic	Static	Dynamic		
Data Flow Transforms	✓	✓	✓	✓	✓	✓
Control Flow Transforms	✓		✓	✓	✓	✓
White-box Crypto	✓	✓			✓	✓
Secure Store	✓	✓	✓	✓	✓	✓
Integrity Verification			✓	✓	✓	✓
Anti-Debug		✓		✓	✓	✓
Code Encryption	✓	✓	✓		✓	✓

CONSIDER SECURITY FROM PRODUCT INCEPTION
AND FACTOR IN UPDATEABILITY

REGULARLY RENEW YOUR SECURITY

CONSIDER THE FULL ATTACK SURFACE

THINK HOLISTICALLY,

THINK EASE OF ATTACK,

THINK MULTI-LAYERED DEFENSE

cloakware™

by irdeto

SECURING DIGITAL ASSETS
FOR 20 YEARS

50 MILLION TRANSACTIONS
PROTECTED PER DAY

MORE THAN 191 MILLION
CRYPTOGRAPHIC KEYS GENERATED
AND UNDER MANAGEMENT

+5 BILLION DEVICES &
APPLICATIONS SECURED

70 MILLION PERSONALIZED
SEMICONDUCTOR CHIPS
PROVISIONED VIA IRDETO'S KEYS &
CREDENTIALS SOLUTION