Cyber inSecurity for Individuals and Enterprises

Mini-School of Global Affairs

Dr. Jesus Borrego
Business School
Jesus.Borrego@ucdenver.edu

About Presenter

- Dr. Jesus Borrego
- School of Business, UC Denver
- PhD in Information Systems Management
- MS Computer Science
- BS Computer Science
- BS Electrical Engineering
- Teaching technology and business courses since 1989

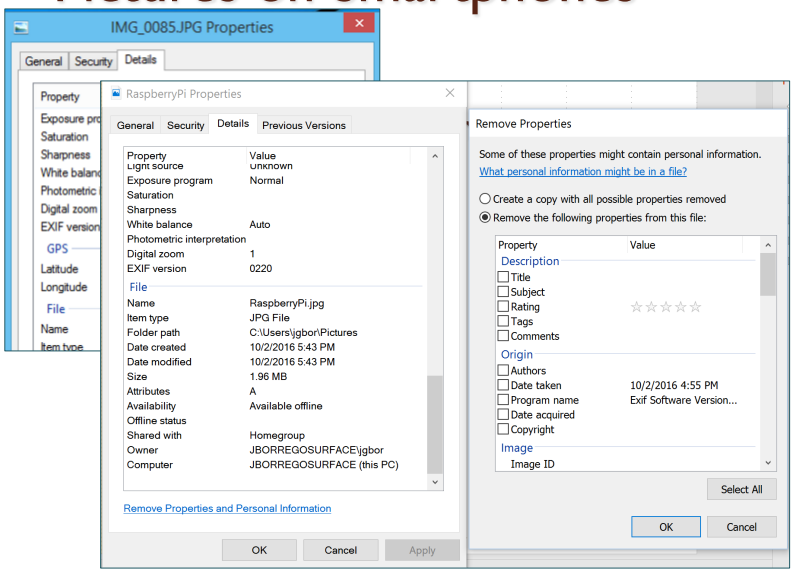
Overview

- CyberSecurity and Privacy in a wired world
- Is Privacy Dead?
- Cyberattacks
- Cyber Fallacies
- Security Measures
- Password hacking
- Information Assurance Workforce
- 100% safe systems

Privacy in a wired world

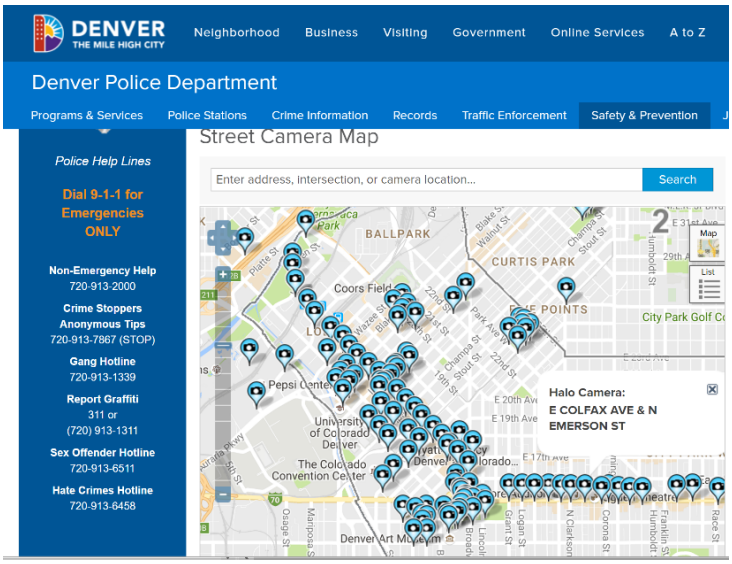
- Webcams on businesses
- Traffic cameras
- GPS on smartphones and cars
- Social Media
- Electronic Records
- Smartphones and tablets
- Financial Institutions, Insurance Companies, Pharmacies

Pictures on Smartphones



Stalkers and GEO information

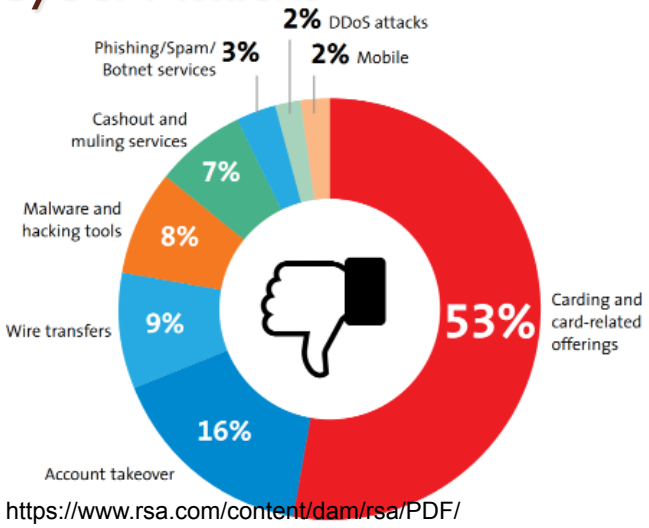
Denver Metro Police Cameras



Privacy is Dead

- Privacy is Dead: The future is fabulous – by Richard Aldrich (16:13 min)
- https://www.youtube.com/watch?v=M11nmdKdKV8

2016 Cyber Attacks



Source: RSA, https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf

Sample attacks

Organization	Date	Records compromised
Banner Health	8/16	3.7M cards
Office Personnel Management	7/15	22.1M
Primera Blue Cross	3/15	11M
Anthem	2/15	80M
Sony Pictures	11/14	Unknown emails
Staples	10/14	1.16M credit cards
Home Depot	9/14	56M cards
JP Morgan Chase	7/14	83M
Community Health System	6/14	4.5M
Michaels Stores	4/14	3M cards
Target	12/13	40M cards, 70M records

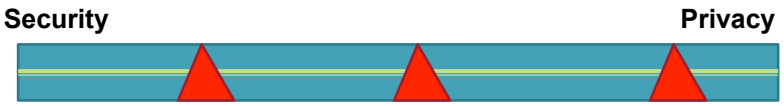
Cyber Security/Privacy Fallacies

- I am not doing anything illegal, I have nothing to hide
- Privacy controls helps authorities monitor and deter terrorists, so I can do with less privacy
- I don't have anything of value, so I am not concerned
- I don't visit unsafe sites, so I am safe

Cyber Security/Privacy Fallacies

- I have a current AV so I am safe
- We do not have money to implement a security plan
- Hackers are not interested in small businesses and individuals
- IT handles our security, so I have nothing to worry about

Security versus Privacy



Retailer Attacks

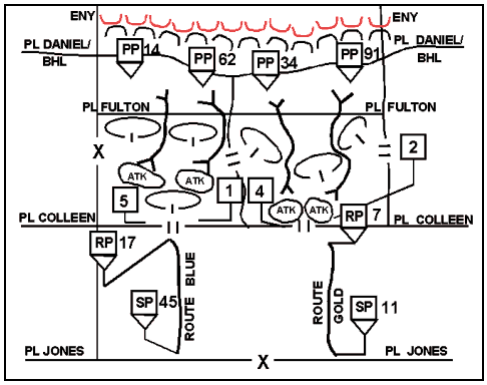
- Multichannel – data captured in many locations
- POS vulnerabilities
- QR Code hacking
- Old technology
- Vulnerable network equipment
- Near Field Communications (Tap to Pay)
- BYOD

Security for Enterprises

- Insider Threats
- Disgruntled employees
- Security Policies
- Background checks for employees
- Hackers
- Virus and Malware
- Social Engineering

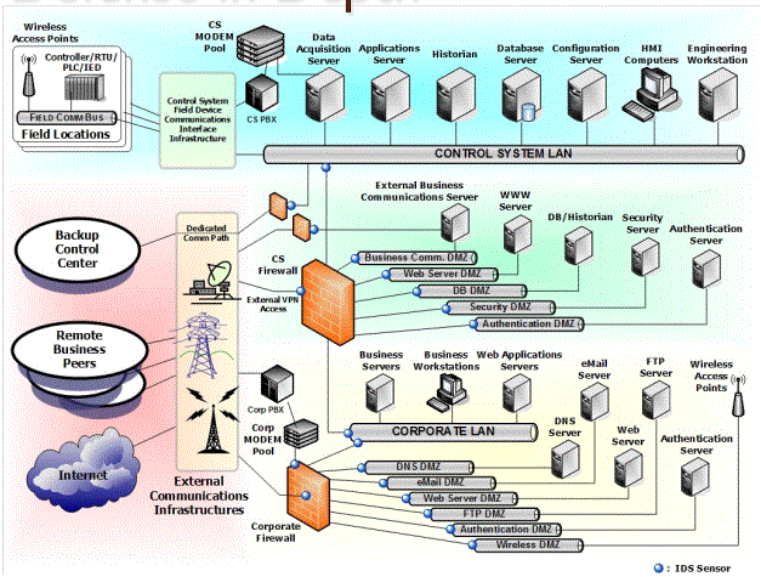
Current Technology

- Security devices are powerful and make it difficult to penetrate at the perimeter



- Layered defense in the military → Defense in Depth

Defense in Depth



Hacking attack

- It is easier to obtain access to the network with social engineering than breaking into the network
- Capturing passwords is easier
- Once you have one password, you get find others until you get the sysadmin

Personal Privacy

- Protect Passwords
- Antivirus
- Firewall
- Application Patching
- WiFi
- Social Engineering

OS Security

- No Operating System is safe
- Apple, Windows, Linux, Android, iOS, Unix – all have vulnerabilities
- What OS has the most vulnerabilities?

2013 Vulnerabilities by OS

Operating system	# of vulnerabilities		# of HIGH vulnerabilities		# of MEDIUM vulnerabilities		# of LOW vulnerabilities	
	2013	2012	2013	2012	2013	2012	2013	2012
Microsoft Windows Server 2008	↑104	48	↑58	35	↑46	12	↓0	1
Microsoft Windows 7	↑100	42	↑55	33	↑45	8	↓0	1
Microsoft Windows Vista	↑96	41	↑53	34	↑43	6	↓0	1
Microsoft Windows XP	↑88	42	↑47	37	↑41	5	●0	0
Microsoft Windows Server 2003	↑86	45	↑46	40	↑40	5	●0	0
Microsoft Windows 8	↑58	5	↑43	5	↑14	0	↑1	0
Linux Kernel	↑158	45	↑15	12	↑119	28	↑24	5
Microsoft Windows Server 2012	↑51	5	↑37	4	↑13	1	↑1	0
Microsoft Windows RT	↑42	2	↑32	2	↑9	0	↑1	0
Apple iOS	↑89	86	↓19	46	↑55	28	↑15	12
Cisco IOS	↓34	36	↓19	23	↑15	10	↓0	3
Ubuntu Linux	↑72	6	↑10	0	↑55	5	↑7	1
Cisco IOS XE	↑23	9	↑16	9	↑7	0	●0	0
Red Hat Enterprise Linux	↑54	2	↑9	0	↑37	1	↑8	1
openSUSE	↑49	0	↑11	0	↑26	0	↑12	0
Apple Mac OS X	↑63	21	↑5	3	↑44	16	↑14	2

Source: http://www.gfi.com/blog/report-most-vulnerable-operating-systems-and-applications-in-2013/

2014 Vulnerabilities by OS

Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

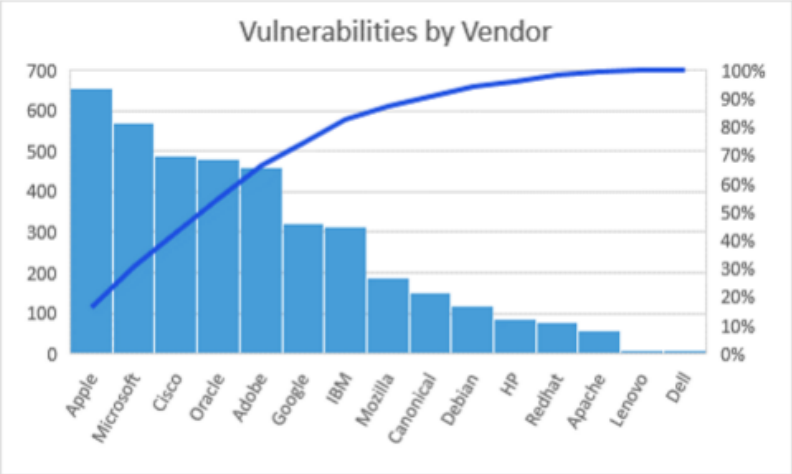
Source: http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/

2015 Vulnerabilities by OS

rank	operating system	number of vulnerabilities
1	Apple OS X	384
2	Microsoft Windows Server 2012	155
3	Canonical Ubuntu Linux	152
4	Microsoft Windows 8.1	151
5	Microsoft Windows Server 2008	149
6	Microsoft Windows 7	147
7	Microsoft Windows 8	146
8	Microsoft Windows Vista	135
9	openSUSE	121
10	Debian Linux	111
11	The Linux Kernel	77
12	Microsoft Windows 10	53
13	Fedora Linux	38
14	Microsoft Windows 2003	36
15	Xen OS	34

Source: http://www.gfi.com/blog/2015s-mvps-the-most-vulnerable-players/

2015 Vulnerabilities



Source: http://www.gfi.com/blog/2015s-mvps-the-most-vulnerable-players/

Mac Vulnerabilities

BUILD

Humbled Apple Admits Hacking After Releasing Removal Tool

BY DAN STEINER | SMALL BUSINESS

Here's a shocking statistic, and one that Apple would NEVER want consumers to know...20% of Mac computers have been infected by some kind of malware.

That's a high number from a company that touts the invulnerability of its OS. Now Apple is disclosing more chinks in its armor. Once Forbes went on record to say Apple is the most valuable company in human history, Apple has done its best to retain that reputation and avoiding any mention of weakness. But it looks like reality is trumping reputation for the tech juggernaut.

Apple Releases Quick Fix

After similar attacks on Facebook, Apple admitted its own systems were infected and released a removal tool a few months ago. This admission was far from a total disclosure of vulnerability. According to the official statement, no information ever left Apple and no real damage was done.

Apparently the attack was startling enough to require an additional software release. Consumers will probably never know, considering Apple's legendary internal security. The company seems founded on the Vegas maxim "What happens on the island, stays on the

Source: https://www.aabacosmallbusiness.com/advisor/humbled-apple-admits-hacking-releasing-removal-tool-020020533.html

iPhone Vulnerabilities

www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html?_r=0

SECTIONS The New York Times

Subpoenas and Gag Orders Show Government Overreach, Tech Companies Argue

Google, Lagging Amazon, Races Across the Threshold Into the Home

Facebook Marketplace Goes Wrong: Sex, Guns and Baby Hedgehogs

TECHNOLOGY

TECHNOLOGY

IPhone Users Urged to Update Software After Security Flaws Are Found

By NICOLE PERLROTH AUG. 25, 2016

SAN FRANCISCO — One of the world's most evasive digital arms dealers is believed to have been taking advantage of three security vulnerabilities in popular Apple products in its efforts to spy on dissidents and journalists.

Investigators discovered that a company called the NSO Group, an Israeli

Source: http://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html?_r=0

Protecting Data

- Password Management
- Multifactor authentication
- Encryption of data in transit, processed, at rest
- Social Engineering awareness

Password Management

- Passwords are entered by the user and stored in the operating system files
- The passwords are hashed before they are stored
- In Windows, the hashed passwords are stored in C:\Windows\System32\config\SAM
  (SAM: Security Account Manager)
- In Linux, in /etc/shadow

Windows passwords

- You cannot access the SAM directory while the system is running
- However, you can boot up with a different OS and access the file
- Even if you can access the file, the passwords are hashed, something like:

Bf08e8473ad3dab10e1ae657b4175361 2ff6bf121bfc32d9d6430ae06af4dbc4

- Passwords are hashed using algorithms such as SHA256

Hashing Advantages

- Knowing the hash value, you cannot recreate the password
- Brute force: try each combination and check the resulting hash.
- For 8 characters:
- AAAAAAAA
- AAAAAAAB
- AAAAAAAC
- … and so on

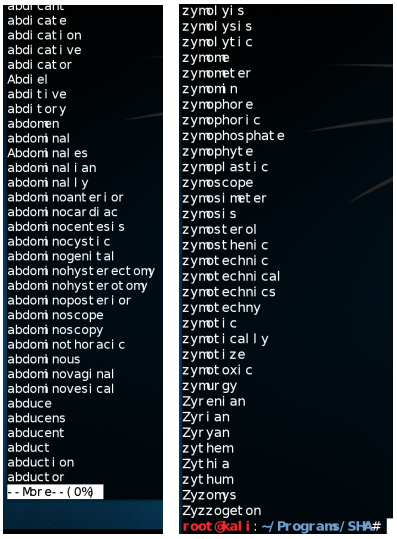
Hashing Advantages (Cont' d)

Characters	Numbers	Length	Combinations
UC or LC	26	8	208,827,064,576
UC and LC	52	8	53,459,728,531,456
UC, LC, #	62	8	218,340,105,584,896
UC, LC, #, SC	72	8	722,204,136,308,736
UC or LC	26	14	64,509,974,703,297,200,000
UC and LC	52	14	1,056,931,425,538,820,000,000,000
UC, LC, #	62	14	12,401,769,434,657,500,000,000,000
UC, LC, #, SC	72	14	100,613,197,241,792,000,000,000,000

Password Cracking

- You can get a dictionary list of words and common passwords
- Add numbers and special characters
- You can then generate the hash for all the combinations and store in a file
- Then, you can obtain the hashed value of a password from the operating system and find the match

Passwords and Hash



Passwords and Hash (Cont'd)

```
zymolysis, 1e3c5fb87ca5af64fb6bfcdcfc444cad2acb17660c0076aec18c03f4983721ed
zymolysis, 3ee5fc1fb366c5f6ca607ba4962123ed9d8e7c27826cfc19cf1554fa1360bb10
zymolytic, 6afad52ecf75e0facc712211b8b014889849d6eb563b6df396c0ceedbd85d144
zymome, 672ba157f72080f8d4c99c681dbc1efabe85828df1abfa38ee009b24c9092cdf
zymometer, 6828c95e8cfb743de49c58fa8e0cee5b2ff0ee3ed65e57d0e094aad7a7ff8355
zymomin, 1d84a822e824b0849f58ec85c14f77a1baa1b83230733d7ff30f6612456df03e
zymophore, 3a835e769bdfd1ef92eddc10172db439f28e14734678ae7b0388e3c7cb90886e
zymophoric, 5c01e1f0305d57413be3e081c1b34c6c87f20f77aade0c890f8a8d2b1d87e1bc
zymophosphate, c632847da47c386f45b4cb3080342fc68129bc7eeb96b4052a59540c23dfe8e1
zymophyte, d670ad3d447d70952d49c0f22f95fb2ebf0f648f4b455c4422b7b03b2e5ad1c1
zymoplastic, 1bf32fe23be8ff4020484b1e0a9706a433de83906413296c9c5dbf4c3ef0f2ae
zymoscope, bdf1b8b8eb8aa2f42a590869fe2bbb7b00f496d176dc829b50cd022c8b56fb28
zymosimeter, 4d158b89d95c229f70f7f3c7c2e3a9cc983205e586e18d3e99dd18663b67e5f0
zymosis, a73085e963b0eb5de2357902ff8e1c4aecb4a92afe52971a1afade4d357ec7c1
zymosterol, 8d63330e74f7ee9d1da4b76a51db3c95a91d6a4494a8f6aba096c7c80fcfc417
zymostheni c, d669186baf8415a160dcaedce6ae66e1f5cf31ad5ccfa0cff67e40d799f0927b
zymotechnic, 6625faddb68ec7015114db61c82a3c8eb17fce1b09935699ec211ce63f1b6c46
zymotechnical, 37e78f9f275374935cd0a495b5b34882776812b63bb65a6513d4397b1c4565dd
zymotechnics, cd807c2dbfa00528aefe22762b7989e1b2f7dbe0a93b977c2ef4acf800b69d5a
zymotechny, 9f34b28b314ab0d53dff505bb169f5830c049149d5ce59279198da6f2103d160
zymotic, 62b37172e6aea0680856b461ec104c2d9a5e7668d6563bd57325055b5bc80762
zymotically, 07205de069b3128180970 0fa716976485dc5d489e1679d51546f2062ff1f1c36
zymotize, 5a94d96c1d8cb98edbf7b9e09e3a994f3242b58fe4cc9fdf8f1cf3e021157f86
zymotoxic, e5f2874021c367b67d694c4cfbd5364dc88bd170abac52759f5e4f7baba63ad0
zymurgy, a6027ea6c6d87a36e17a5e59e6710c100350a14e27d060e2e49c972356e74cf2
Zyrenian, 743132b159df86dd236a25212bfc70fc5ce0dad7e983188b1057a135093c938d
Zyrian, 3cbbd228eb0027f9f135b54436a9004c95b149d5a1a2ffa9194e1c4a53b827d1
Zyryan, 8250dc68854fab0b1b58f65d637810c1d85f277e4fc349a109920c754451aa96
zythem, d01b84ab9f8802843b1b786168701b847450054f73921a0754685733a54077fc
Zythia, 664642b08cced8ea3f9093e64ae47248eac4b152f76705aa7a3f6fa63fbb7b0b
zythum, e86874ade6fa7309b7d634ee45348e588b81d912a9a65a8f395b1e4af773dae7
Zyzomys, b4daa3bf439466fa74f5c87fcb8b3e726e17a6ccb1dc10f34a3d861b53273564
Zyzzogeton, 6ba4f070804a746d768c07d80ce8627cfe0ee3100edd8ecfd728e5c413ef9f0f
root@kali: ~/Programs/SHA#
```

Program to generate hash

GNU nano 2.5.1 File: main.cpp

```
{
  string aLine, output1;

  ifstream inFile;     //input file handle
  ofstream outFile;    //output file handle

  // open files
  inFile.open  ( "words.txt"    );
  outFile.open ( "SHA_File.txt" );

  if (inFile )            //test for proper open of input file
  {
    // process file
    while ( getline ( inFile, aLine ) )
    {
      output1 = sha256 ( aLine );
      cout  << aLine << "\t\t\t sha= " << output1 << endl;
      outFile << aLine << "," << output1 << endl;
    }//end of while
    // close files
    inFile.close  ( );
    outFile.close ( );
    cout  << endl  << "SHA File created! " << endl;

  }//if
  else
    cout  << "error opening input file "  << endl;

return 0;
```


Password Cracking

- RainbowTables exist with millions of hashed passwords
- Finding the password requires us to search the file for a match in the hash and we get the password

Linux Demo

Information Assurance Opportunities

- IA expected growth 18-37% (to 2024)
- Needs:
  - Incident handling and response
  - Analytics and Intelligence
  - Security Information and Event Management
  - Access and Identity Management
  - Application Security Development
  - Advanced Malware Prevention
  - Cloud Computing/Virtualization

Top Areas for IA Professionals

- Banking/Finance/Insurance
- Information Technology/Management
- Government (Defense)
- Government (Non Defense)
- Consulting/Professional Services

Occupational Outlook

OOH HOME | OCCUPATION FINDER | OOH FAQ | OOH GLOSSARY | A-Z INDEX | OOH SITE MAP | EN ESPAÑOL

OCCUPATIONAL OUTLOOK HANDBOOK

Search Handbook Go

Computer and Information Technology >

Information Security Analysts

EN ESPAÑOL PRINTER-FRIENDLY

Summary | What They Do | Work Environment | How to Become One | Pay | Job Outlook | State & Area Data | Similar Occupations | More Info

Summary

Quick Facts: Information Security Analysts	
2015 Median Pay	$90,120 per year $43.33 per hour
Typical Entry-Level Education	Bachelor's degree
Work Experience in a Related Occupation	Less than 5 years
On-the-job Training	None
Number of Jobs, 2014	82,900
Job Outlook, 2014-24	18% (Much faster than average)
Employment Change, 2014-24	14,800

Information security analysts work to protect a company's computer systems.

What Information Security Analysts Do

Information security analysts plan and carry out security measures to protect an organization's computer networks and systems. Their responsibilities are continually expanding as the number of cyberattacks increases.

Work Environment

Most information security analysts work for computer companies, consulting firms, or business and financial companies.

Source: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Most Secure Computer

- Characteristics of the 100% secure computer:

Raspberry Pi