

# Cooking Cybersecurity

**Why we all need new recipes to be successful**

Olivier Ménil  
Business Development Manager Security

# About me



More than 20 years in security (in various functions including technical ones 😊)

- I have a passion about (cyber) security & I like cooking!
- Experience in start-up, own company, integrators & vendors
- National and international speaker for Security Conferences
- No criminal record (yet)!



# Agenda

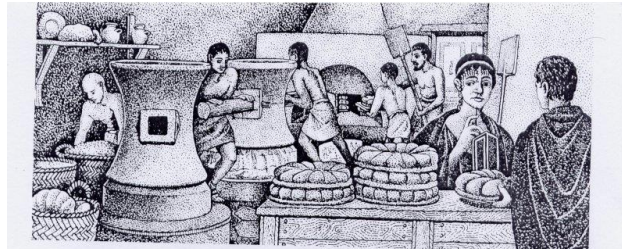
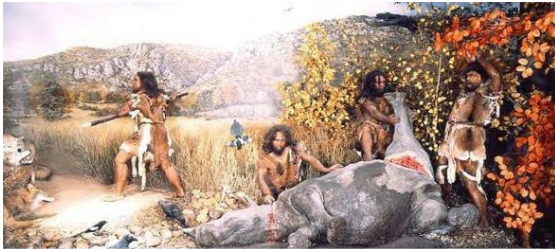
- **Setting up the scene**
- **How to (learn to) cook ?**
- **Why cooking and cybersecurity have so much in common ?**
- **Examples**
- **Conclusion**

# Setting up the scene



# Setting up the scene

- Cooking is very old and is a critical component of mankind!



# Setting up the scene



- Cybersecurity is not that old but think about the CIA principle ... especially the C!

**700 BC Scytale**  
The Spartan military used scytale to send messages during times of battle. Both sender and receiver had a wooden rod of the exact diameter and length. To encrypt a message, the sender tightly wound a piece of leather or parchment around the stick and wrote a message on it. The sender tightly wound it to the receiver, who could only read the message once it was tightly wound around his own scytale. Anyone else would see disarranged letters with no meaning.

**1467 Alberti cipher**  
Leon Battista Alberti invented and patented the first polyalphabetic substitution cipher, changing the cipher of every given letter. The Alberti cipher was composed of two metal discs on the same axle, one inside the other, which revolved around alphabets and variable rotators.

**1797 Jefferson wheel**  
Invented by Thomas Jefferson while he was George Washington's secretary of state, the wheel consisted of 26 cylindrical wooden pieces, three inches in length. The letters of the alphabet were inscribed on the edge of each wheel and rotated until turning them would scramble and unscramble words. This concept would spawn the code machine in Turing times and then look for the one line of letters that made sense. The U.S. Army used this cryptograph device again between 1902 and 1942.

**1943 Enigma machine**  
Building on the work of British cryptanalysts, Bletchley Park's main decryption establishment during WWII – was on deciphering the Enigma machine, a series of related electro-mechanical rotor cipher machines used by the Axis powers. It was considered unbreakable, as the Nazis changed the cipher every day. The Bletchley Park team, which included the father of modern computing, Alan Turing, capitalized on the machine's one fundamental flaw: The letter could be encrypted as itself. Armed with this information and Turing's Bombe machine, which greatly reduced the time required to crack Enigma, pretty soon the Allied forces knew the Wehrmacht's secret moves.

**1961 First computer password**  
Developed by MIT's CTSS (Compatible Time-Sharing System), when computer time was scarce, extremely expensive and limited to research institutions, CTSS employed the first password and username method of user authentication. Although this was the first system to experience a password breach. In 1966, a software bug landed on the system that allowed users to see its master password file, so that anyone who logged in was presented with the file and all its passwords.

**1979 DES invented**  
The National Bureau of Standards invented DES (Data Encryption Standard) using 56-bit of encryption. At the time, it was so strong, not even super computers could crack it. Indeed, DES was the standard for almost 20 years – until the Electronic Freedom Foundation broke the DES key in 56 hours in 1998. A year later, they reduced that time to just over 22 hours.

**1985 Videocipher II**  
HBO, Comcast, and others began using a TV satellite scrambling system (called Videocipher II). DES called Videocipher II, making site-right scrambling of heavy used TV content moves the platform of an entire generation. A tremendous black market emerged for descramblers, and six years after TV scrambling technology's debut, it was estimated that only 20% of dish owners were paying subscribers.

**1995 "Hackers"**  
The cult classic introduces the mainstream to just-coming computer viruses, and gets at hacking culture. As the computer world starts heating up, and data encryption becomes ever more relevant.

**1997 AES is developed**  
The National Institute of Standards and Technology developed AES (Advanced Encryption Standard), which is still used today. 128-bit encryption takes 2 to the 50th power (or 2.580 years) to crack. A device that could crack a billion billion (10<sup>18</sup>) AES keys per second (if such a device could ever be made) would require about 3607.75 years to exhaust the 256-bit key space. (That's 174,445,211,009,100,366,087,763,708 years.)

**1997 CAPTCHA**  
As online spam grew, AkivaVista chief scientist Andre Broder and his colleagues developed a filter that generated images of random text that machine vision systems cannot read. Through Turing tests, in 2000, Luis van Arman at Carnegie Mellon updated the concept with extra layers of security that made it more evolved spam and hacking practices. With ReCAPTCHA, users became even harder for machines to read. Thanks to increased awareness and feature-like lines running through the text.

**2006 Rise of identity theft**  
Hacking and identity theft became big business as more and more people join the Internet, adding increasingly large amount of personal data to the web. One of the largest data thefts in recent times took place on networks belonging to the T.J. Maxx and Marshall's department stores, as many as 45 million credit and debit card numbers were stolen between 2006 and 2007, highlighting how hackers can breach decrypted data networks.

**2009 State-sponsored hack**  
Although never proven, the Chinese government is blamed for attacks that breached the security of Silicon Valley companies like Google and Yahoo and their users.

**2011 Year of the hacker**  
Advanced Persistent Threats (APTs) emerged – well-funded, coordinated groups of hackers pursuing specific agendas. 70 million Sony PlayStation users were hacked; so were 200,000 Citibank customers. Facebook revealed that 600,000 of its accounts were being compromised each day. And 2012 promises to be more of the same. This January, Zippos was hacked in a big way. 24 million customers' names, e-mails, phone numbers, addresses, and partial credit card numbers were exposed.

**2012 Personal data lockers**  
Personal data lockers have emerged as a way to make the most of the Internet while remaining safe. By centralizing storage of personal data – from payment information and passwords to ID numbers and receipts – in one locally-encrypted place that only the user can access. The data is as secure as possible, while remaining conveniently under his or her control. No one else can decrypt the data – not even the purveyors of the technology or the government can get to it. In a sense, personal data can now go wherever a user wants it to go, but nowhere else.

# How to (learn to) cook ?



# How to (learn to) cook ?

- The basic elements for cooking are obvious:
  - Ingredients
  - Tools
  - Location / facilities
  - Recipes
  - ... but please don't forget the most important!





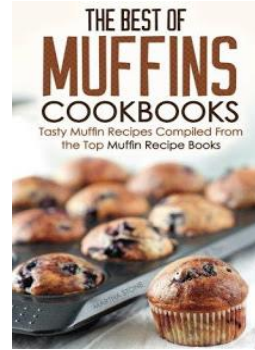
How to (learn to) cook ?

The Chef



# How to become a chef ?

- There are key elements to be successful:
  - Learning
  - Training
  - Testing
  - Passion
  - Accept failures and challenges
  - Bottom up approach (stay humble)



# Why cooking and cybersecurity have so much in common ?



# Why cooking and cybersecurity have so much in common ?

- In fact all previous elements can be easily compared:
  - Ingredients & tools -> devices
  - Location & facilities -> infrastructure / connectivity / datacenter / cloud
  - Recipes -> configuration and policies
  - Cooks -> Cybersecurity specialists
  - Training -> training
  - Tasting -> auditing / pentesting
  - Dressing -> finetuning

# How cooking and cybersecurity have so much in common ?

- Furthermore ... even the way how cooking is regulated in a professional kitchen can be compared:



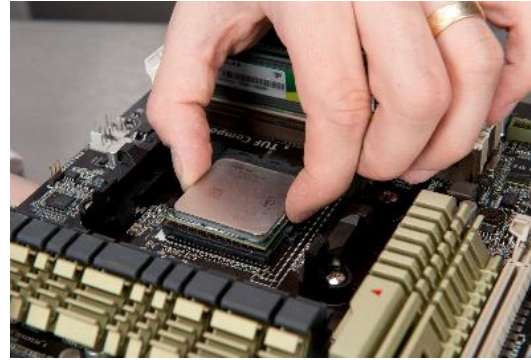
- Clear roles and responsibilities
- Segmentation, risk control and management

# Examples



# State of the art / best of breed / industrialisation

- Cooking is like cybersecurity: “standardized” or “à la carte”



# Implementation / configuration

- It MUST be precise, accurate, exact .... In fact perfect!
- Why do you think in cybersecurity we all like to use ... cookbooks?

**SING LITTLE ALICE**  
*Marble Pound Cake*

There was a time in Philadelphia, not too long ago, that every wedding cake vendor was pushing chocolate chip cake. I get why—a hint of chocolate within a vanilla cake is appealing—but I just don't think chocolate chips are the best way to achieve that result. We attempted to find a balance by creating this vanilla and chocolate swirl cake. It takes a bit of work, because it requires making two cake batters and then swirling them together, but it's worth the extra effort.

*Serves:* 15 to 20 people

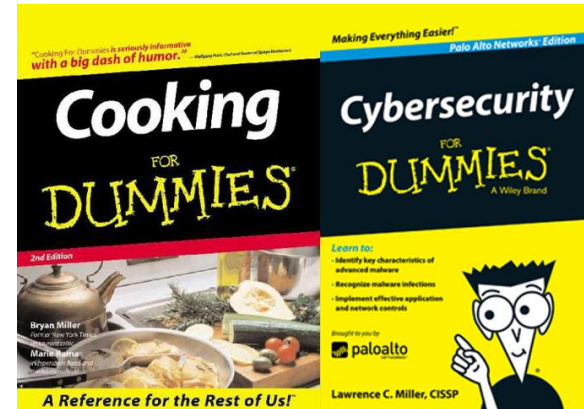
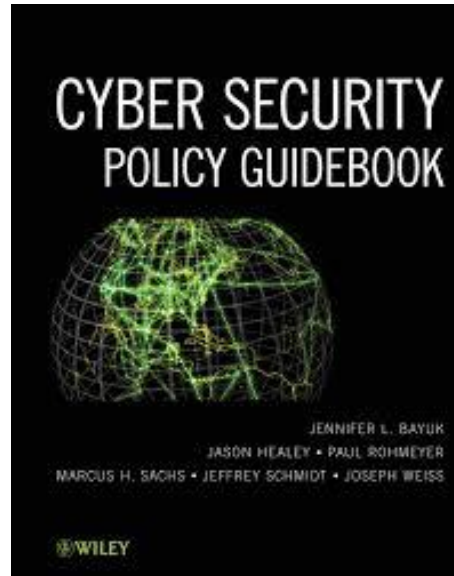
- 1 Preheat the oven to 350°F. Coat three 9-inch round cake pans with vegetable shortening, line the bottoms with parchment paper, and spray with nonstick cooking spray.
- 2 Make the vanilla batter first. In a medium bowl, whisk together the flour, salt, baking powder, and baking soda.
- 3 In the bowl of a stand mixer fitted with the paddle attachment, beat the butter and sugar on medium speed until light and fluffy, scraping the bowl as necessary, about 3 minutes. Add the eggs, 1 at a time, beating until blended and scraping the bowl as necessary. Add the vanilla and rum extracts and beat until blended.

*continued on the following page*

*Setup time:*  
60 minutes  
*Total time:*  
1 hour and 30 minutes

Vegetable shortening  
Nonstick cooking spray  
with flour

**VANILLA BATTER**  
4 cups cake flour  
¾ teaspoon regular salt  
¼ teaspoon baking powder  
¼ teaspoon baking soda  
3 sticks (1½ cups)  
unsalted butter, at room  
temperature  
3 cups granulated sugar  
8 large eggs  
1½ teaspoons pure vanilla  
extract  
¼ teaspoon pure rum  
extract  
1 cup sour cream





# Old ingredients ... New recipes

- Modern cooks like to (re)use forgotten ingredients
- ... it's exactly the same for cybersecurity!



# Remember ... Logs?

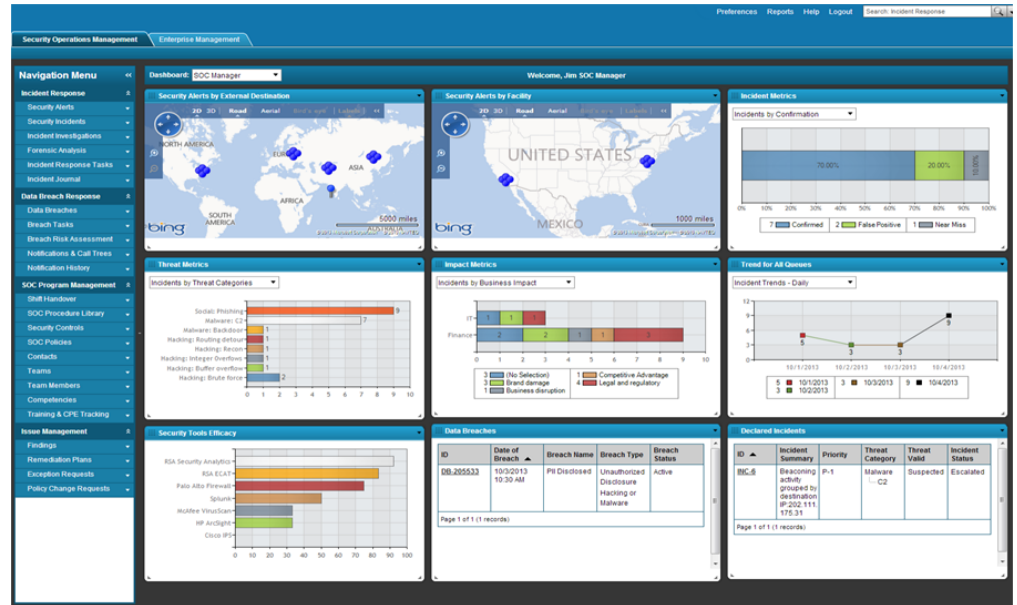
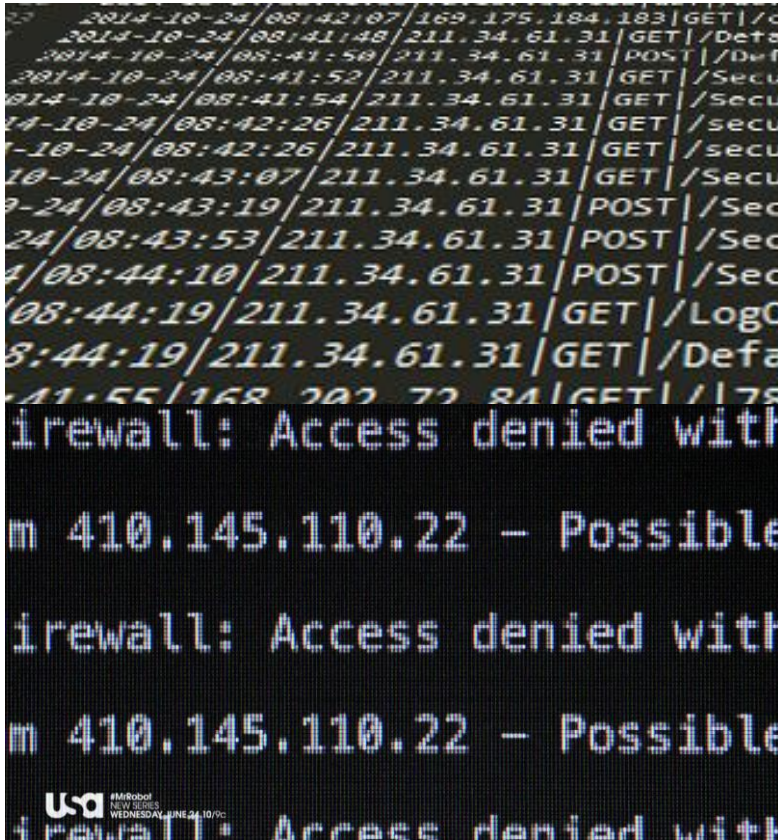
- What was told to us in the 90's ?



3	Log Reduction	* Any	* Any	* Any Traffic	NBT UDP bootp UDP rip	drop	- None	R70J-A	* Any	this rule helps the LOG files to be tidier by deliberately not logging RIP,bootp and NBT
4	* Any	* Any	* Any Traffic	NBT TCP microsoft-ds	drop	- None	* Policy Targets	* Any	There are always some WP* hosts around...which shouldn't fill the log	
5	Cleanup Rule	* Any	* Any	* Any Traffic	* Any	drop	- None			



# Logs ... today ... everywhere ... for everything!



# Conclusion



# Still not convinced?

